**Instituto Tecnológico de Costa Rica**

**Escuela de Ingeniería en Electrónica**

# Elaboración de un prototipo para un sistema integral de seguridad en el Instituto Costarricense de Electricidad

**Informe de Proyecto de Graduación para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura/Bachillerato**

**Francilena Garro Navarro**

**Cartago, 26 de Noviembre de 2009**

**INSTITUTO TECNOLOGICO DE COSTA RICA**

**ESCUELA DE INGENIERIA ELECTRONICA**

**PROYECTO DE GRADUACIÓN**

**TRIBUNAL EVALUADOR**

Proyecto de Graduación defendido ante el presente Tribunal Evaluador como requisito para optar por el título de Ingeniero en Electrónica con el grado académico de Licenciatura, del Instituto Tecnológico de Costa Rica.

Miembros del Tribunal

Ing. Sergio Morales Hernández

Profesor lector

Ing. Juan Carlos Jiménez Robles

Profesor lector

Ing. Francisco Navarro Henriquez

Profesor asesor

Los miembros de este Tribunal dan fe de que el presente trabajo de graduación ha sido aprobado y cumple con las normas establecidas por la Escuela de Ingeniería Electrónica

Cartago, noviembre de 2009



1

Declaro que el presente Proyecto de Graduación ha sido realizado enteramente por mi persona, utilizando y aplicando literatura referente al tema e introduciendo conocimientos propios.

En los casos en que he utilizado bibliografía, he procedido a indicar las fuentes mediante las respectivas citas bibliográficas.

En consecuencia, asumo la responsabilidad total por el trabajo de graduación realizado y por el contenido del correspondiente informe final.

Cartago, noviembre de 2009

Francilena Garro Navarro

Céd: 1-1229-779



2

## Resumen

Este proyecto se desarrolló con el fin de integrar el control de intrusión que utilizaba un sistema de alarmas con monitoreo telefónico y el control de acceso implementado con el Sistema de Gestión Andover Continuum, con los que cuenta el Instituto Costarricense de Electricidad. La configuración del sistema original presentaba una falta de comunicación entre ambos controles y un desaprovechamiento de las capacidades del sistema Andover. El diseño e implementación se realizó basándose en la plataforma Andover y sus dispositivos. Para esto se elaboró un prototipo del sistema de seguridad integral, que permitió la realización de pruebas y análisis. La implementación del sistema a escala real permitirá aumentar la seguridad en las instalaciones y el prototipo construido se utilizará para el entrenamiento del personal.

## Abstract

This project was developed to integrate the two systems for intrusion control that the Instituto Costarricense de Electricidad (ICE) has, one system uses alarms and phone monitoring and the other one is an access control implemented using the Andover Continuum System. Configuration on the original platform had a lack of communication between both control systems and wastage of capabilities of the Andover system. Design and implementation was based on the Andover platform and its devices. A prototype of the integrated security system was made in order to do different tests and analysis. Implementation of the actual system will increase the security in the buildings and the prototype developed will be used to train the staff.

## Dedicatoria

*A mis padres Jorge y Lorena que me han guiado y acompañado en este recorrido.*

*A mi hermana Loreana que ha estado conmigo en todo momento.*

## Agradecimiento

Agradezco al Ing. Homer Elizondo Orozco por haberme brindado la oportunidad de desarrollar este proyecto en el Departamento de Seguridad Electrónica del ICE.

Al Ing. Antonio Ramírez Bogantes por su guía y colaboración en el desarrollo del proyecto.

A mis compañeras y compañeros del departamento de Seguridad Electrónica, Rosaura, Silvia, Ana, Jacquelin, Mileidy, Patricia, Allan, Randall, Ariel y a todos los demás, por su apoyo y colaboración.

A mis amigos Esteban Zúñiga, Sebastián Jiménez, Diana Korte, Kendall Picado, Gloriela Rodríguez, José Daniel González y Jorge Hidalgo.

A un agradecimiento especial a Natalia Cerdas.

# ÍNDICE GENERAL

# INDICE DE FIGURAS

## ÍNDICE DE TABLAS

# Capítulo 1. Introducción

El Instituto Costarricense de Electricidad es una de las instituciones más representativas de nuestro país, que a lo largo de su trayectoria ha innovado con tecnologías de punta tanto en electrificación como en telecomunicaciones.

Hechos actuales como la entrada en vigencia del TLC con los Estados Unidos y con ello la apertura en el mercado de telecomunicaciones se traducen, en una nueva serie de retos y cambios que el ICE debe enfrentar para lograr mantener el nivel competitividad, ante empresas que ingresen al país a ofrecer estos servicios. Los cambios que se avecinan involucran diversas áreas, entre las que se debe incluir la seguridad, la cual marca uno de los pilares para el desarrollo de toda empresa.

Más específicamente se tratará en este proyecto la seguridad de la infraestructura, mediante los dispositivos de acceso e intrusión y una plataforma de seguridad electrónica.

## 1.1. Problema existente e importancia de su solución

El ICE cuenta con diferentes procesos y departamentos con información y equipos de gran costo económico, los cuales requieren altos niveles de seguridad para garantizar su protección.

El análisis se realizó tomando como base uno de los edificios de oficinas del ICE, en las cercanías del Gimnasio Nacional en Sabana Sur. Consta de un sistema de control de acceso que se comunica con una plataforma de seguridad electrónica (ANDOVER) y de forma independiente, dispositivos de alarmas contra intrusos monitoreados vía telefónica, como se muestra en la figura 1.1.

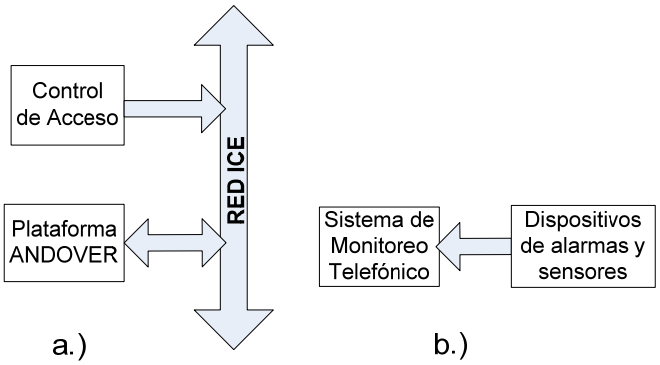



Figura 1.1 Diagramas del sistema actual, a.) Sistema de Control de Acceso. b.) Dispositivos de alarmas monitoreados vía telefónica.

La utilización de alarmas y sensores es parte esencial dentro del sistema de seguridad requerido, al igual que los controles para determinar los sectores, las restricciones y prioridades.

El sistema de monitoreo telefónico, aunque poseía cierto nivel de sectorización, no contaba con definición de prioridades y restricciones, además, presentaba una serie de desventajas, como la necesidad del ir al sitio para modificaciones, mantenimiento, y verificaciones, impidiendo evaluar de otra forma falsas alarmas o situaciones que afectaran el correcto funcionamiento de los dispositivos.

Por otra parte, para evitar el ingreso de personas ajenas a la institución, se tenía un sistema de control de acceso el cual estaba ligado a la red del ICE y utilizaba la plataforma de seguridad electrónica ANDOVER.

La plataforma ANDOVER, permitía dentro de sus funcionalidades el manejo de otros dispositivos, entre los que destacan aquellos utilizados en los sistemas de alarma y vigilancia, sin embargo, se disponía de esta solo para los controles de acceso.

Lo anterior demostró que la principal desventaja se encontraba en la falta de comunicación directa entre ambos sistemas y la subutilización de la plataforma de seguridad electrónica.

## 1.2. Solución seleccionada

Debido a la necesidad de un sistema único que permitiera una interacción entre las alarmas y el control de acceso, utilizando la plataforma de seguridad ANDOVER, se propuso el desarrollo de un prototipo en el cual se simularan las diversas conexiones de acuerdo a los requerimientos y necesidades del sistema de seguridad.

El prototipo consistió en un módulo de pruebas que mostraba los tres escenarios en que se ha utilizado el control de acceso, así como la conexión de los dispositivos de entrada y salida para las alarmas, de forma tal que fuera posible evaluar la capacidad de los controladores que utiliza la plataforma, además de la interacción con los módulos, todo esto mediante el desarrollo de una aplicación para la atención de eventos.

# Capítulo 2. Meta y Objetivos

## 2.1. Meta

Crear un prototipo que sea una base para el establecimiento de un sistema de seguridad que unifique el control de acceso y las alarmas, permitiendo una mayor utilización de los controladores y dispositivos de la plataforma de seguridad.

Indicador: Un mayor aprovechamiento en las funciones de los controladores utilizados por la plataforma.

## 2.2. Objetivo general

Diseñar un prototipo que integre el control de acceso y las alarmas, en un sistema de seguridad único, que permita simular los diferentes eventos y la respuesta que se brinde a cada uno de ellos.

Indicador: Aumentar el número de dispositivos y eventos ligados al control de seguridad, de manera que se mejore el aprovechamiento del potencial de la plataforma utilizada.

## 2.3. Objetivos específicos

1. Diseñar un módulo con todos los dispositivos que se están utilizando actualmente y otros dispositivos para realizar las pruebas de compatibilidad e integración.

Indicador: Determinar cuáles son los dispositivos que pueden ser interconectados al sistema.

2. Valorar el hardware del sistema, los sensores, alarmas y controladores actuales, para determinar los parámetros eléctricos y de comunicación.

Indicador: Determinar los parámetros especificados en la **Tabla 4.1** del procedimiento metodológico.

3. Diseñar y optimizar una aplicación para la integración del control de acceso, los lectores de proximidad, sensores y dispositivos de alarmas.

Indicador: Determinar los dispositivos que pueden integrarse e interactuar en el sistema propuesto.

4. Desarrollar las políticas y los escenarios de las acciones del control de las alarmas integrado al control de acceso.

Indicador: Definir los privilegios de utilización, sectorización y control de la alarma.

# Capítulo 3. Marco teórico

El proyecto consistió en la realización de un prototipo para la evaluación del funcionamiento y capacidad de la plataforma de seguridad utilizada, de manera que fuera posible la integración de los controles de acceso y alarmas, para mejorar el rendimiento del sistema y el alcance del mismo. Para esto fue necesario conocer el concepto del sistema de seguridad, la plataforma de seguridad y los dispositivos que se utilizaron durante el diseño y desarrollo del proyecto.

## 3.1. Descripción del sistema de seguridad, control de acceso y alarmas de intrusión.

El sistema de seguridad como tal debe proveer los medios necesarios para garantizar la protección tanto cuando el personal se encuentre presente como el tiempo en que las instalaciones puedan permanecer desocupadas.

El objetivo de un sistema de seguridad automatizado se orienta a la integración de funcionalidades de software y hardware en un control único que permita atender la mayoría o si es posible la totalidad de las necesidades demandadas, las cuales buscan el control total del ingreso y salida de personas así como el monitoreo continuo de las diferentes áreas. Existen dos pilares fundamentales en un sistema de seguridad, el acceso y la intrusión

Un control para el acceso de personal es imprescindible dentro de un sistema de seguridad, ya que brinda la posibilidad de conocer quienes entran y salen y si hay personas ajenas a la institución o sin autorización que intenten ingresar en áreas restringidas. En un sistema de seguridad automatizado, por medio de una base de datos que interactúa con el software y el hardware de control de acceso instalado, es posible establecer los permisos y las restricciones para el personal

que labora en el edificio según las funciones e incluso limitarlo de acuerdo a horarios.

Estos controles de acceso se deben colocar en áreas específicas, y varían su configuración según la ubicación o la funcionalidad, dependiendo de los niveles de seguridad requeridos. Existen zonas en donde es necesario conocer la identidad de quien entra y quién sale, un ejemplo de esto son las puertas de acceso principal, en donde como función adicional es posible monitorear el cumplimiento de las horas laboradas por los empleados al conocer el momento de su ingreso y salida, al igual que en ubicaciones que requieran altos niveles de seguridad. Otras configuraciones registran únicamente la identidad de la persona que ingresa, ya que en la salida utilizan dispositivos como sensores o interruptores que lo habilitan pero no lo identifican.

La intrusión hace referencia a personas no autorizadas que intentan ingresar en ciertas áreas fuera de los horarios permitidos o que son restringidas. Se basa en el monitoreo continuo de estas áreas por medio de redes de sensores de movimiento ubicados de acuerdo a su rango de alcance y monitoreados por controles que verifican el estado de estos para identificar posibles eventos. Estos sistemas utilizan un panel para el control, el arme o desarme del sistema, así como los dispositivos sonoros para las alarmas.

El monitoreo de las redes de sensores se puede realizar a través de sistemas con líneas telefónicas, o bien en el caso de los sistemas de seguridad automatizados empleando controladores y módulos que por medio de redes internas enlazan los sistemas a nivel de software permitiendo recibir las alarmas en las estaciones de trabajo, identificando los sectores en donde se produjeron, adicionalmente en estos sistemas es posible la interacción entre los controles de acceso y de intrusión, ampliando sus funciones como por ejemplo la utilización del control de acceso para el arme y desarme de las alarmas prescindiendo de la utilización del panel.

## 3.2. Descripción técnica de los dispositivos de hardware y software más relevantes que intervienen en el diseño del prototipo sistema integral de seguridad.

**Sistema de gestión de edificios Andover Continuum**

Andover Continuum es una interacción de software y hardware diseñado para monitorear y controlar las funciones en una edificación. Estas funciones incluyen seguridad, control de acceso, iluminación, ventilación, acondicionamiento de ambientes, entre otras, sin embargo no esta limitado a estas. El hardware consiste en controladores de red, interfaces de entrada y salida; el software incluye el programa CyberStation y la base de datos.

El software encargado de la comunicación, monitoreo y control del sistema Andover Continuum se conoce como CyberStation. Este es una aplicación basada en Windows que se corre desde la estación de trabajo e interactúa con el sistema, provee la interfaz gráfica que permite desplegar y manipular los datos, el ajuste de horarios, alarmas y permisos, control de puertas y personal entre otros. A través de CyberStation es posible configurar el hardware y programar las rutinas de control en los controladores de red, así como las aplicaciones en la estación de trabajo para la atención de eventos, por medio del lenguaje de programación Plain English. Andover Continuum. Otra parte fundamental a nivel de software es la base de datos que almacena la información pertinente para el sistema de automatización, describe la estructura y operación del edificio, los puntos de evaluación del sistema, selección de límites de las variables monitoreadas, configuración del hardware, datos del personal y toda la información necesaria para el funcionamiento del sistema.

Andover Continuum Cyberstation es un sistema basado en los principios de la programación orientada a objetos. Las clases y los objetos son las partes

fundamentales del sistema. Así como, los atributos de los objetos y la relación entre estos de acuerdo a la jerarquía dentro de una red física.

El diseño del sistema Andover Continuum está basado en la escalabilidad, es decir que es posible la configuración de grandes redes y múltiples estaciones de trabajo con un único servidor con el software MS SQL para la base de datos Continuum.

**Componentes del sistema:**

- Network Controllers.
- Módulos de entrada/salida (AC-1, DI8, DO-4R)
- Estaciones de trabajo.
- Software Cyberstation
- Base de datos

El lenguaje de programación Plain English reconoce dos tipos de objetos los que están basados hardware (Controladores, estaciones de trabajo, puntos de entrada/salida) y los que se basan en software (variables de sistema y atributos), adicionalmente estos objetos se agrupan en clases. Al crear el objeto CyberStation reconoce el nombre y el alias del mismo, la diferencia está en que el nombre del objeto es almacenado en la base de datos continuum y no en el controlador, por otra parte el alias es almacenado en ambos.

El nombre puede contener un máximo de 64 caracteres, mayúsculas o minúsculas, números, (_ . / -) y espacios. Por otra parte el alias puede tener como máximo 16 caracteres, debe comenzar con una letra, caracteres alfanuméricos, ( _ . ), sin espacios y sin palabras reservadas, keywords o (+, -, /, *).

Los atributos de cada objeto que hacen referencia a las características del mismo son utilizados en los programas de Plain English. Además, algunos de

estos atributos pueden ser modificados a través de la línea de comandos de la estación de trabajo.

**Programación en Plain English**

Cada línea se conoce como instrucción o declaración y puede tener un máximo de 132 caracteres. Así mismo, un grupo de instrucciones puede ubicarse bajo una etiqueta ya sea con la palabra LINE antes de la etiqueta o el nombre de la etiqueta seguida por ( : ). La etiqueta puede tener un máximo de 16 caracteres, incluyendo (_ . ) y números.

Las “keywords” son palabras que reconoce el controlador y sirven para construir las instrucciones. Estas palabras se dividen en tipos ya sean declaraciones, funciones, operadores, variables locales, variables de sistema o constantes del sistema.

La línea de comandos es un área de CyberStation que permite ejecutar manualmente comandos de Plain English.

Los programas pueden ser de dos tipos, Looping o Fall Thru dependiendo de la forma en que se desea ejecutar, en el primer caso el programa va a evaluar las variables hasta que se cumplan las condiciones requeridas para continuar con las instrucciones siguientes, en el otro caso las instrucciones se ejecutan en forma secuencial independientemente del cumplimiento de las condiciones que le anteceden.

Los programas Fall thru pueden iniciar de acuerdo al estado de un punto especifico o variable del sistema. Esto se configura en el cuadro de dialogo de atributos de la variable respectiva, se selecciona Triggers y se agrega a la lista que aparece en el editor el programa que se desea ejecutar.

### Proceso de escaneo del sistema

El sistema de control continuum continuamente ejecuta un proceso de escaneo. Cada controlador posee un intérprete interno que se encarga de reunir los datos necesarios para la ejecución del próximo escaneo a través de todos los programas, leer y ejecutar una línea por cada programa habilitado, iniciando por el primero de la lista de ejecución, convertir y habilitar las salidas.

El proceso de escaneo está determinado por 6 etapas que se realizan en forma secuencial:

1. Actualiza y ejecuta todas las variables del sistema.
2. Actualiza los horarios.
3. Actualiza los puntos de entrada del controlador.
4. Ejecuta los programas y las líneas de comandos.
5. Actualiza los puntos de salida del controlador.
6. Procesa todas las alarmas y de ser necesario actualiza la barra de estados en la pantalla principal del CyberStation.

El controlador posee un mecanismo que evita que un solo programa monopolice el proceso de escaneo, por lo que si se trata de ejecutar más de 5000 declaraciones en una misma línea durante un escaneo, va a ocurrir un error en el sistema.

### Controlador de red NetController II

El controlador utilizado es el NetController II CX9940, con soporte para 32 módulos de entrada/salida; posee un microprocesador Motorola MCF5275 @ 150MHz, con una memoria flash de 32MB y 128 MB DDR SDRAM, cuatro puertos de comunicación programables, utiliza el protocolo IP y se comunica vía Ethernet con la estación de trabajo Andover Continuum.

El NetController II puede ser configurado utilizando el lenguaje Andover Continuum Plain English, se programa a través de la estación de trabajo, utilizando el software CyberStation de Andover, y el controlador lo almacena y ejecuta.

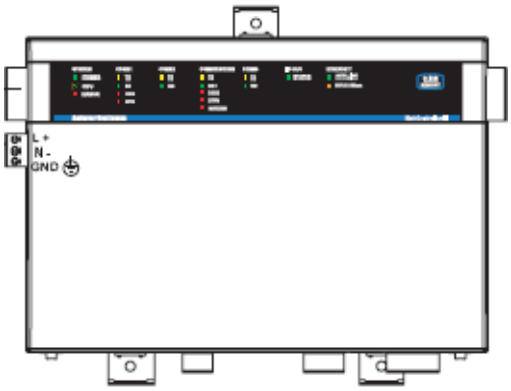



Figura 3.1. NetController II, Andover Continuum. (10)

El microprocesador del NetController II posee un sistema operativo que consiste en el boot loader, application firmware y software adicional. En el caso de que exista una nueva versión del sistema operativo es posible actualizarlo por medio del *Update OS* en el cuadro de edición del *InfinityController*.

**Módulos de control de acceso AC-1**

Los AC-1, son módulos especializados para el control de acceso, permiten monitorear a distancia los lectores de proximidad y las puertas, con bajo costo de cableado y agrupados en un control central. Su función principal es establecer la comunicación entre los dispositivos del control de acceso y el NetController donde se encuentra el firmware supervisor de control de acceso. Durante la operación normal las decisiones del control de acceso se toman en el módulo de base de datos en el CPU del NetController de Andover Continuum, el cual provee almacenamiento de hasta 75000 registros personales en forma local.

Cada AC-1 está diseñado para el control de una puerta y puede ser configurado para permitir la entrada por medio de una tarjeta de proximidad, una

tarjeta con un pin de acceso o por medio de teclado, además la rutina de operación de la puerta puede ser modificada a través de programas en el lenguaje Plain English.

| Connection | Description |
|---|---|
| ⏚ | Earth Ground |
| 1. | Reader +V |
| 2. | Reader GND |
| 3. | Reader DATA (Wiegand I) |
| 4. | Reader CLK (Wiegand 0) |
| 5. | Reader LED |
| 6. | Sup Input Aux |
| 7. | Sup Input Door |
| 8. | Sup Input REX |
| 9. | Sup Input RETURN |
| 10. | Door NC |
| 11. | Door NO |
| 12. | Door COM |
| 13. | OUT2 NC |
| 14. | OUT2 NO |
| 15. | OUT2 COM |

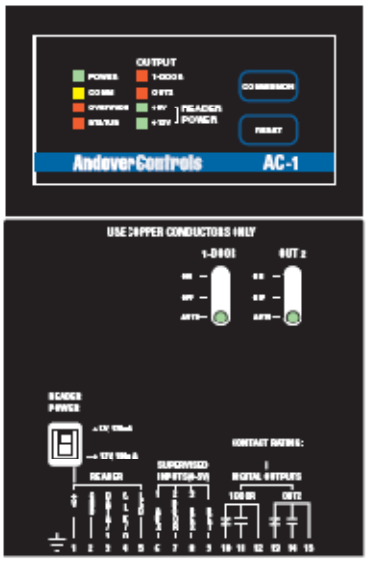



Figura 3.2. Módulo de control de acceso AC-1 con sus entradas y salidas indicadas. (4)

Estos módulos cuentan con las entradas destinadas a la conexión de los lectores de tarjetas de proximidad Wiegand de hasta 64 bits, asimismo se provee la alimentación requerida por los lectores, la cual se puede seleccionar entre 5V o 12V. Adicionalmente, poseen tres entradas de alarma supervisadas, las cuales determinan su estado de acuerdo al valor de la impedancia en cada una de ellas (Figura 3.2). Las entradas se utilizan para monitorear el estado del contacto magnético de la puerta, los dispositivos de solicitud de salida o cualquier otro dispositivo de alarma de dos o tres estados (on-off-trouble) y pueden ser programadas.

Las entradas del AC-1 requieren de una configuración específica en el circuito de entrada para que los estados sean reconocidos correctamente, estas configuraciones y los estados que representan en cada una se muestran en la Tabla 3.1.

**Tabla 3.1** Configuración del circuito de entrada en el AC-1.[1]

| Conexión | Interruptor | Valores de resistencias (KΩ) | Valor en la entrada |
|---|---|---|---|
| NC Serie | Cerrado | 10 | Off |
| | Abierto | ∞ | On |
| | Cortocircuito | 0 | Trouble |
| | Circuito abierto | ∞ | On |
| NO Serie | Abierto | ∞ | Off |
| | Cerrado | 10 | On |
| | Cortocircuito | 0 | Trouble |
| | Circuito abierto | ∞ | On |
| NC Paralelo | Cerrado | 0 | Off |
| | Abierto | 10 | On |
| | Cortocircuito | 0 | Off |
| | Circuito abierto | ∞ | Trouble |
| NO Paralelo | Abierto | 10 | Off |
| | Cerrado | 0 | On |
| | Cortocircuito | 0 | On |
| | Circuito abierto | ∞ | Trouble |
| NC Serie-Paralelo | Cerrado | 5 | Off |
| | Abierto | 10 | On |
| | Cortocircuito | 0 | Trouble |
| | Circuito abierto | ∞ | Trouble |
| NO Serie-Paralelo | Abierto | 10 | Off |
| | Cerrado | 5 | On |
| | Cortocircuito | 0 | Trouble |
| | Circuito abierto | ∞ | Trouble |

Las salidas del AC-1 son dos relé SPDT o tipo C de 24VAC/DC @ 5A. Una de las salidas está destinada para la apertura de la puerta y la otra es una salida adicional que puede ser utilizada para alarma. Cada salida posee un interruptor que permite el control manual o bien el control por medio software.

**Lector de proximidad HID MiniProx Wiegand 5365**

El HID MiniProx es un lector de tarjetas de identificación por radiofrecuencia, posee una frecuencia de transmisión y excitación de 125KHz, por lo que se dice que es un lector de baja frecuencia. Además utiliza el protocolo Wiegand para la comunicación con los dispositivos del control de acceso, que le permite un alcance de hasta 150m en la conexión entre los dispositivos.

El lector MiniProx reconoce más de 137000 códigos únicos, requiere una alimentación de 4,75V-16V(DC) y puede identificar tarjetas a una distancia entre 5cm y 15 cm según la tarjeta utilizada.

**Tarjeta de proximidad HID ISOProx II**

La tarjeta HID ISOProx II está basada en la tecnología de identificación por radiofrecuencia, transmite a 125KHz y puede ser programada por este medio.

Esta tarjeta posee un rango de lectura estable, que no se ve afectado por las condiciones ambientales o por cualquier tipo de obstrucciones. Puede ser leída por un lector HID MiniProx, desde una distancia de 12.5cm y está disponible para más de 137000 de códigos únicos lo que permite una alta confiabilidad en cuanto a la identificación y seguridad.

**Módulo de entrada DI8**

Los DI8 son los módulos de entradas digitales de Andover Continuum que se utilizan principalmente para el monitoreo de sensores. Poseen ocho entradas

digitales que pueden ser programadas por software, las cuales monitorean las señales de 0 a 5v.

Las 8 entradas de este módulo, figura 3.3, pueden ser utilizadas como contadores de baja frecuencia, 10Hz, adicionalmente para los canales 1 y 2 los contadores pueden tener una frecuencia máxima de 10KHz.

| Connection | Description |
|---|---|
| ⏚ | Earth Ground |
| 1. | IN 1 |
| 2. | IN 2 |
| 3. | RETURN |
| 4. | IN 3 |
| 5. | IN 4 |
| 6. | RETURN |
| 7. | IN 5 |
| 8. | IN 6 |
| 9. | RETURN |
| 10. | IN 7 |
| 11. | IN 8 |
| 12. | RETURN |


Figura 3.3. Módulo de entradas DI8. (4)

**Sensores de movimiento y proximidad**

Los sensores utilizados son el RTE1000 Request to Exit y el detector pasivo infrarojo RX-40PT.

El RTE1000 Request to Exit, es un sensor óptico utilizado en dispositivos de accesos. Requiere de 12V o 24V de alimentación y posee un alcance de 2,3m de altura, con un rango máximo de 1,5m y un rango mínimo de 0,8m. La salida del sensor esta dada por un relé SPDT o de tipo C cuya duración se puede seleccionar entre 5, 30, 75 y 125 segundos.

El RX-40PT es un detector de movimiento óptico, con un alcance de 12mX12m, cuya salida es un relé N.C.

### Módulo de salida DO-4R

Los módulos DO-4R, figura 3.4, contienen 4 salidas de relé programables tipo C 240VAC @5A. Las salidas uno y dos y la tres y cuatro se pueden combinar si se requiere para obtener salidas de tres estados.

| Connection | Description |
|---|---|
| ⏚ | Earth Ground |
| 1. | OUT 1 NC |
| 2. | OUT 1 NO |
| 3. | OUT 1 COM |
| 4. | OUT 2 NC |
| 5. | OUT 2 NO |
| 6. | OUT 2 COM |
| 7. | OUT 3 NC |
| 8. | OUT 3 NO |
| 9. | OUT 3 COM |
| 10. | OUT 4 NC |
| 11. | OUT 4 NO |
| 12. | OUT 4 COM |

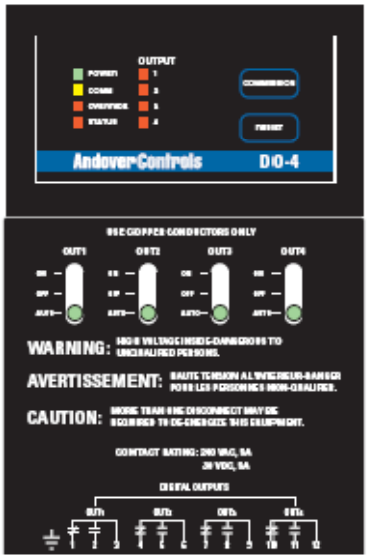



Figura 3.4. Módulo de salidas DO-4R. (4)

## 3.3. Descripción de los principales principios electrónicos relacionados con el prototipo del sistema de seguridad integral

### Automatización de edificios

La teoría de automatización de edificios, o lo que se conoce como edificios inteligentes, propone la integración de las diferentes conexiones eléctricas en un control único. La conexiones eléctricas hacen referencia tanto a lo indispensable que es la iluminación, electrificación y sistemas motrices, como a los sistemas de audio, video, circuito cerrado de televisión, acondicionamiento de los ambientes, comunicaciones, alarmas contra incendio, de intrusión, bombas y sistemas pluviales eléctricos, puertas y accesos, entre estos.

La optimización en el control comienza con la integración e interacción de los diferentes sistemas, lo que permite el manejo de las condiciones internas y externas de la edificación, en busca de confort y seguridad para los ocupantes y tomando en cuenta el ahorro energético, que se traducen en mejoras en la productividad y satisfacción.

**Protocolo de comunicación Wiegand**

Este protocolo nació de la necesidad de comunicar los lectores de tarjetas Wiegand a los dispositivos de control de acceso. La comunicación se establece a través de tres líneas, una por la que se envían los unos lógicos, DATA1, otra por la que se envía los ceros lógicos, DATA0, como se observa en el diagrama de la Figura 3.5 y la tercera línea corresponde a la conexión de tierra, GND.

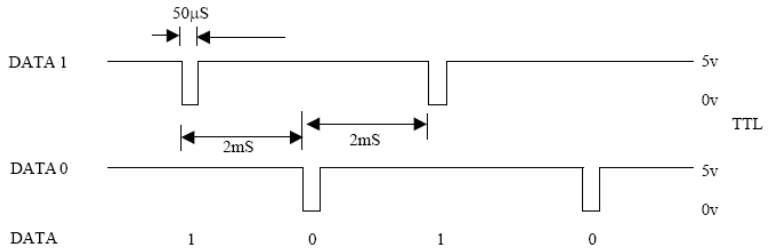



Figura 3.5. Diagrama de tiempos de transmisión de secuencia de bits 1010. Protocolo Wiegand. (8)

Las líneas DATA1 y DATA0 permanecen en alto (5V) durante el tiempo en que no haya transmisión, si se requiere transmitir un bit 1 se envía un pulso por la línea DATA1 que cambia su estado a bajo (0V) por aproximadamente 50µs y luego vuelve a alto, si por el contrario se requiere enviar un bit 0 el pulso es enviado por la línea DATA0 con la misma duración; entre un pulso y otro se da una separación de 2ms.

**Identificación por radio frecuencia (RFID)**

La tecnología de identificación por radiofrecuencia, utiliza las ondas de radio para almacenar y transmitir datos. Este sistema consta de dos partes

fundamentales, las tarjetas RFID o tanspondedores y los lectores RFID o transceptores. Una de las ventajas que ofrece esta tecnología es que no requiere de una línea de visión directa para la lectura de las tarjetas.

Los sistemas RFID trabajan en las bandas de frecuencia de 125KHz o 134KHz para baja frecuencia y 13.56MHz para alta frecuencia.

**Tarjetas RFID o transpondedores**

Las tarjetas RFID están formadas por una antena, un transductor y un circuito integrado, que posee la memoria interna que almacena los datos para la identificación. La capacidad de la memoria varía de acuerdo al modelo y la función que vaya a desempeñar la tarjeta. Al existir memorias de solo lectura y de lectura y escritura, se tienen diferentes variaciones en las de tarjetas; las de solo lectura que poseen un código de identificación único que se establece durante la fabricación, las de lectura y escritura, que permiten modificar la información de identificación y un tipo especial de etiquetas, anticolisión que le permite al lector identificar varias tarjetas al mismo tiempo.

**Tipos de tarjetas**

La alimentación utilizada por las tarjetas, define a su vez el tipo de tarjetas, según sea pasiva, semipasiva o activa.

*Tarjetas pasivas:* Este tipo de tarjetas no poseen una fuente de alimentación propia y utiliza la energía inducida de la señal de escaneo del lector para generar una pequeña corriente que le permite operar, enviando de regreso la señal de radiofrecuencia para la identificación. Este tipo de tarjetas utiliza el backscatter sobre la portadora, es decir que la antena recibe la señal, obtiene la energía y la transmite a la vez, al mismo punto donde se originó, en este caso el lector RFID, como se muestra en la figura 3.6.

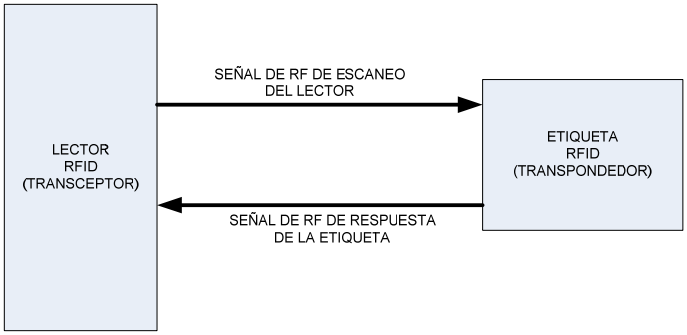



Figura 3.6. RFID, backscatter.

Las tarjetas pasivas tienen un alcance promedio que va desde los 10 cm aproximadamente hasta algunos metros, dependiendo de la frecuencia de operación y la función que cumplen. Una ventaja adicional al tipo alimentación, es el costo de fabricación el cual es menor con respecto a los otros tipos de tarjetas.

*Tarjetas semipasivas:* La alimentación en este tipo de etiquetas es proporcionada por una batería que se utiliza para alimentar el circuito integrado. De igual forma la energía proporcionada por la señal del lector se emplea para la señal de respuesta que se transmite de regreso al lector, sin embargo al disminuir los requerimientos de energía, es posible optimizar las antenas para un rango de transmisión mayor.

*Tarjetas activas:* En este caso las tarjetas contienen una fuente de alimentación propia, esta característica les permite transmitir señales con mayor potencia, lo que se traduce en un mayor alcance de la señal con respecto al lector hasta varios cientos de metros, 500m aproximadamente, así como una mayor eficiencia de transmisión en entornos como el agua y el metal. Sin embargo son más caros, de mayor tamaño y generalmente con una vida útil menor.

Por otra parte este tipo de tarjetas permite almacenar información enviada por el transceptor, además de contener sensores de registro para diferentes variables.

### Lector RFID o Tranceptores

El lector RFID o transceptor incluye una antena, un transceptor y un decodificador. El lector continuamente envía señales para monitorear la presencia de alguna tarjeta, al detectar alguna decodifica la información y la envía a los dispositivos encargados de procesarla.

# Capítulo 4. Procedimiento metodológico

## 4.1. Reconocimiento y definición del problema

En el Instituto Costarricense de Electricidad existe el departamento de Seguridad Electrónica de la Dirección de Protección y Seguridad Institucional, que se encarga de la seguridad y protección de las instalaciones y los empleados de la institución.

Este departamento tiene a su cargo el desarrollo e implementación de los sistemas que se utilizan para estos fines entre los que destacan el control de acceso y las alarmas de intrusión, que actualmente se mantienen como sistemas independientes.

Para el control de acceso se ha utilizado la plataforma de seguridad Andover que posee el potencial de ser utilizada como sistema de intrusión, sin embargo sus funcionalidades se encontraban disminuidas principalmente debido al desconocimiento del lenguaje de programación y la configuración del sistema.

Por otra parte la independencia del sistema de control de acceso y el de intrusión, redujo los niveles de seguridad y dificultaba las acciones de mantenimiento y atención de eventos principalmente en el caso del sistema de intrusión, el cual correspondía a un sistema de alarmas con monitoreo telefónico.

## 4.2. Obtención y análisis de información

El primer paso en el diseño del sistema consistió en el análisis y conocimiento del control de acceso y la plataforma de seguridad. Se realizó una visita al centro de control en el Edificio Central en Sabana Norte, en donde se encuentra el personal encargado de la atención de las alarmas y los módulos que contienen los controladores y dispositivos instalados para el control de acceso. Además se recorrieron algunos de los ductos de la instalación.

Posteriormente se investigaron las características eléctricas de estos dispositivos, así como de otros afines para determinar compatibilidades con la plataforma. Además, se accesó a una de las estaciones de trabajo para conocer el funcionamiento básico de la plataforma Andover Continuum.

## 4.3. Evaluación de las alternativas y síntesis de una solución

La solución se planteó como la posibilidad de integrar el control de acceso y la etapa de intrusión en un sistema único, capaz de soportar ambas funcionalidades y que permitiera la interacción de estos.

El sistema de seguridad desarrollado permitiría el arme y desarme de las alarmas de intrusión a través del control de acceso, así como el monitoreo por medio de las estaciones de trabajo, lo que otorgaría al sistema una redundancia tal que sería posible la verificación de los eventos y el análisis de los mismos para la toma de decisiones y acciones respectivas.

Debido a la existencia de la plataforma de seguridad ya instalada, con un alto costo y subutilizada, la solución presentada, involucraba el aprovechamiento de las características y las funcionalidades de esta plataforma en la atención de los eventos. Se propuso el desarrollo y diseño de un módulo prototipo que simulara los diferentes escenarios y tuviera conexión con la base de datos, para observar el comportamiento real del sistema y así valorar la ejecución de las aplicaciones programadas, los sensores, los tiempos de respuesta, el monitoreo, las conexiones y compatibilidades, proporcionando los medios para un análisis que permitiera el mejoramiento y la optimización del sistema de seguridad.

## 4.4. Implementación de la solución

La implementación del prototipo se llevó a cabo en dos etapas. La primera de ellas contempló el diseño del módulo de pruebas. Se analizaron las características eléctricas de los diferentes dispositivos de la plataforma a utilizar,

tabla 4.1, los controladores, las fuentes, los dispositivos de acceso y de entrada o salida, además de los lectores y los sensores, entre otros, todo esto a través de pruebas de laboratorio y de la información contenida en los manuales y hojas de datos correspondientes.

**Tabla 4.1.** Parámetros de evaluación de hardware.

| Parámetro a evaluar | Resultado esperado |
|---|---|
| Nivel de tensión de salida de los sensores (V) | Los niveles de tensión de entrada de los controladores y niveles de tensión de salida de los sensores deben ser compatibles entre ellos. |
| Nivel de tensión de entrada en los controladores (V) | |
| Corrientes de entrada y salida de los sensores (A) | Las corrientes de entrada y salida de ambos dispositivos deben ser compatibles entre ellos. |
| Corrientes de entrada y salida de los controladores (A) | |

La siguiente etapa se centró en el estudio del lenguaje de programación Plain English, y la configuración de los dispositivos, para la correcta interacción con la base de datos y el máximo aprovechamiento de la plataforma. Se desarrollaron las rutinas de software para el control y la interacción del sistema de control de acceso e intrusión, permitiendo la comunicación directa entre los sensores y los dispositivos de ingreso, determinando los diferentes eventos y por tanto las acciones para cada uno de acuerdo a los diferentes escenarios simulados en el módulo de pruebas.

## 4.5. Reevaluación y rediseño

El prototipo del sistema de seguridad como herramienta de pruebas, dio la oportunidad de conocer el sistema, así como parte del alcance y potencial de la plataforma. Una vez concluido el diseño propuesto, pasó a ser un medio de análisis y estudio del sistema para conocer nuevas necesidades que pudieran surgir y mejoras posteriores. Para esto el módulo diseñado contempló la posibilidad de conectar dispositivos diferentes a los utilizados para realizar las pruebas correspondientes y analizar su compatibilidad.

La capacitación es otro aspecto que formó parte del prototipo terminado, ya que se incluyó como parte de los medios utilizados para la instrucción de los técnicos y el personal que trabaje con la plataforma. El manual final incluyó todos los aspectos técnicos de hardware y software necesarios para tal fin.

# Capítulo 5. Descripción detallada de la Elaboración del prototipo para el sistema integral de seguridad

La elaboración del prototipo del sistema integral de seguridad constó de dos etapas. La primera de estas etapas involucró el diseño e implementación a nivel de hardware del módulo de pruebas. La segunda etapa implicó el desarrollo de las aplicaciones y la programación del controlador, según los diferentes requerimientos del sistema, para el análisis de funcionalidad y factibilidad.

## 5.1. Análisis de soluciones y selección final

El sistema se pretendió como una solución ante la poca o nula comunicación entre los sistemas de control de acceso y de intrusión existentes. Lo que se buscaba era que através de la red de control de acceso fuera posible el arme y desarme de las alarmas, la verificación de eventos y el control del personal que entrara y saliera de un área determinada, elevando los controles de seguridad. Por ello se inició con el conocimiento de los escenarios o situaciones en que se aplicaran los controles de acceso, ya fuera en las puertas principales de los edificios o bien puertas para zonas específicas como oficinas y bodegas, de los que se tomaron 3 casos específicos que fueron implementados en el módulo de pruebas.

El primero de ellos se utilizaba fundamentalmente en puertas principales y contaba con la identificación por medio de la tarjeta de proximidad tanto en la entrada como en la salida de la misma, el segundo y tercer caso se encontraban en oficinas, constaba de identificación en la entrada por medio de la tarjeta de proximidad y utilizaba un dispositivo de solicitud de salida, ya fuera un interruptor o un sensor de movimiento respectivamente.

El nuevo sistema debía ser capaz de llevar un control exacto del número de personas que entraban y salían de un área específica, tomando en cuenta la

validez del acceso y la ejecución del ingreso o la salida. La identificación se daría a través de lectores y tarjetas de proximidad ligados a los dispositivos de acceso que procesaran la información obtenida. Era necesario que el control tomara en cuenta no solo una identificación que validara el acceso, sino debía condicionarse a un reporte adicional del ingreso, ya fuera a través de hardware, software o una combinación de ambos, con lo que se pretendió establecer una política según la cual todo el personal debía identificarse al entrar a un área, tal medida aumentaría el control del personal que trabajaba en dicho espacio.

La salida al igual que la entrada debía ser registrada, sin embargo el procedimiento a seguir tendría que incluir tanto el conteo de personas por el control de acceso, como el monitoreo por medio de sensores de movimiento, lo que implicaba una interacción entre los dispositivos de intrusión y de acceso, especialmente en los casos en que no existía identificación a la salida, ya que esto le restaba confiabilidad al conteo, debido a que no era posible conocer el momento de salida de cada persona que hubiera ingresado, de esta forma el monitoreo otorgaría la redundancia que permitiría conocer la actividad dentro del área y compararla con los contadores para decidir las acciones con que el sistema respondería.

Los accesos contaban con alarmas en los casos en que la puerta permanecía abierta por un tiempo mayor al permitido o fuera abierta de manera forzosa, mediante aplicaciones de software que facilitaron la interacción y la configuración de los dispositivos, para así generar las acciones de respuesta como una alarma sonora local, un registro del evento en la base de datos y además una notificación en el centro de control por medio de las estaciones de trabajo, en cualquiera de los casos, de manera tal que la situación pudiera ser controlada con los medios correspondientes.

Adicionalmente el conocimiento de la permanencia del personal por medio del control de acceso y el monitoreo, permitía armar y desarmar los dispositivos que

formaban parte del sistema de intrusión, de forma sectorizada, de acuerdo a las necesidades del personal y los horarios de acceso establecidos.

Una vez que el sistema de intrusión se encontraba activo, cualquier movimiento o actividad que fuera detectada se reportaría al centro de control por medio de las estaciones de trabajo y se activarían de forma local los dispositivos sonoros y visuales correspondientes al área afectada. Si en el momento de activación del sistema se detectaba movimiento y el contador de dicha área indicaba que no había personal registrado, se activaría una alarma de prevención indicando que una o más personas permanecían dentro sin autorización, en caso contrario se activarían las alarmas del sistema de intrusión.

Las situaciones y escenarios que se describieron se reunieron en un prototipo que facilitó el análisis y la evaluación de los diferentes eventos. La diferencia entre el prototipo y la implementación del sistema real radicaba en la cercanía de los dispositivos, ya que el montaje en un único modulo de pruebas permitió el análisis y evaluación de los diferentes eventos, así como los posibles problemas de implementación y diseño que se pudieran presentar y por tanto las correcciones necesarias para la depuración y obtención de un sistema óptimo.

El prototipo planteado debió contemplar los diferentes escenarios en que oportunamente se utilizaría el sistema, por lo que los componentes utilizados para su diseño debían ajustarse a las necesidades reales, ya que no pretendía ser solo un ejemplo de la implementación del sistema sino una herramienta fiable para el desarrollo del mismo en mayor escala, es decir en las edificaciones que conforman la planta física del ICE, en las diferentes ubicaciones tanto dentro como fuera del área metropolitana.

## 5.2. Descripción del hardware

El módulo de pruebas debió contener tanto los dispositivos para el control de acceso con las conexiones que se requerían evaluar, como los dispositivos necesarios para el control de intrusión. Parte de los requisitos del sistema era que se continuara con la utilización del Sistema de Gestión Andover que manejaba los accesos, motivo por el cual los componentes utilizados para la implementación así como los circuitos de simulación debieron ser compatibles con este.

El Sistema de Gestión Andover Continuum ha sido la plataforma utilizada para los controles de acceso. Esta tiene la capacidad de integrar diversas funciones de automatización y es utilizada en el desarrollo de edificios inteligentes, sin embargo hasta ese momento sus funciones estaban limitadas únicamente al sistema de acceso debido al desconocimiento de las funciones y el lenguaje que permitiera la explotación del potencial de la plataforma.

Por otra parte, la solución que se planteó demostró que el sistema de intrusión, que hasta ese instante se había utilizado, quedaba excluido y se partió del control de accesos ya existente para el diseño y desarrollo del sistema integral, en parte debido al potencial de la plataforma y al costo de la misma.

El diagrama de la Figura 5.1 muestra la distribución del módulo de pruebas utilizado para el desarrollo del prototipo del sistema integral de seguridad. Para la facilidad de la comprensión del sistema, se dividió en bloques de acuerdo a la funcionalidad o situación que se estaba evaluando. Al respecto se tienen cuatro bloques, el primero de ellos es el bloque de control, el segundo y tercero correspondieron a los bloques del control de acceso y finalmente el bloque de entradas y salidas para los dispositivos del control de intrusión.


Figura 5.1 Diagrama de bloques del módulo de pruebas del prototipo del sistema integral de seguridad

**Bloque de control**

El bloque de control era la unidad central del sistema, estaba conformado por el controlador de red NetController II y la fuente de 24V que este requería para funcionar. El NetController II adicionalmente proveía los pines en el conector de comunicación que facilitaban la alimentación para los módulos que se ligaran a este o bien se podía utilizar una fuente adicional.

El controlador fue programado utilizando el software CyberStation desde la estación de trabajo por medio del puerto de Ethernet RJ-45 10/100MB. Los controladores y el software se comunican mediante una red IP y para esto era necesario introducir la información de la dirección de forma que CyberStation pueda establecer la comunicación.

**Bloque Puerta 1**

El prototipo debía contener los tres casos de conexión del control de acceso, dos de ellos eran con identificación en la entrada y la diferencia estaba en el dispositivo utilizado para la salida. Estos casos se agruparon en el bloque Puerta1.

En la etapa de entrada de este bloque se utilizó un lector de proximidad de frecuencia de transmisión de 125KHz, con protocolo Weigand y tarjetas de identificación por radiofrecuencia. La salida de este bloque requirió probar la respuesta del control ante dos posibles dispositivos, un interruptor o un sensor de solicitud de salida RTE 1000.

La configuración de salida utilizada permitía realizar la conexión en el mismo módulo de control de acceso AC-1 en que se tenía conectado el lector de proximidad, ya que en un mismo módulo existen las entradas para un lector y un dispositivo de salida, sin embargo, dado que la prueba estaba orientada a dos tipos diferentes de dispositivos de salida se utilizó un AC-1 adicional para la conexión del segundo dispositivo como se observa en la Figura 5.2.

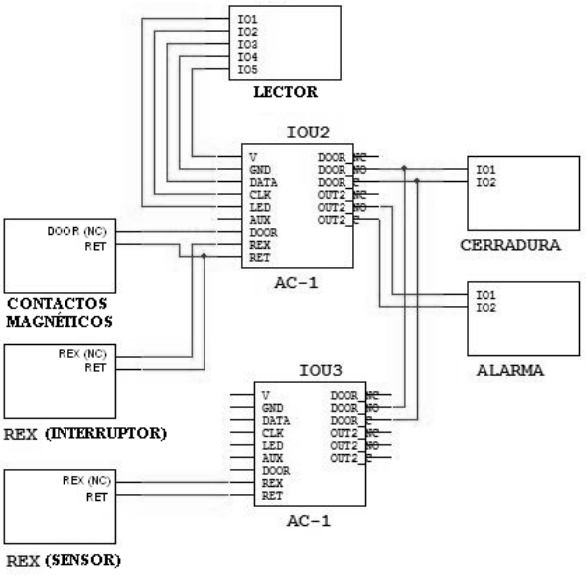



Figura 5.2 Diagrama de conexión de los módulos de la Puerta 1.

Los pines del 1 al 5 del AC-1 estaban destinados a la conexión del lector, de ellos 1 y 2 eran las salidas de alimentación con dos tensiones 5V y 12V seleccionables, para el lector HID MiniProx se utilizaron 5V. Las entradas de datos 0 y 1 requeridos por el protocolo Weigand se encontraban en los pines 3 y 4, además una línea para el led del lector en el pin 5. Esta conexión se hizo en el primer AC-1 del bloque Puerta 1.

En este mismo AC-1 se conectó el circuito de prueba que simulaba los contactos magnéticos en los pines 7 y 9, así como el interruptor de salida en los pines 8 y 9, siendo el pin 9 el común. La conexión debió realizarse de esta forma debido a que cada una de las entradas estaba definida para una función específica que solo podía ser modificada y manipulada por el software. Se utilizaron dos de las entradas, la restante era la entrada auxiliar en el pin 6, que en esta aplicación no se utilizó.

La configuración de las resistencias en las entradas del AC-1 era de gran importancia, debido a que monitoreaba el cambio en la impedancia de los circuitos en las entradas para determinar el estado, ON/OFF. Existen diferentes conexiones que se observan en la Tabla 3.1, de las que se utilizó la configuración NCSerie-Paralelo, ya que poseía la ventaja de que reconocía únicamente los estados del interruptor abierto y cerrado como ON y OFF, si por alguna razón existía un corto circuito o un circuito abierto lo registraba como un estado indefinido, trouble.

Las resistencia utilizadas en la configuración debieron ser de 10KΩ, de acuerdo a los requerimientos del AC-1, colocadas una en paralelo con los pines de entrada y otra en serie con el dispositivo, como se muestra en la Figura 5.3, correspondiente a la conexión con un sensor o interruptor de salida. Esta configuración se debió utilizar en todas las entradas, incluyendo la auxiliar y la de los contactos magnéticos.

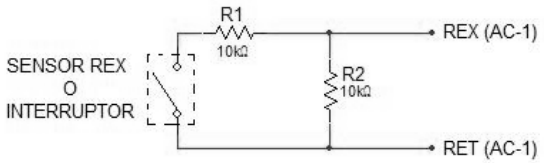



Figura 5.3 Circuito NCserie-paralelo para las entradas del AC-1.

En el bloque Puerta 1, los contactos magnéticos que normalmente se utilizan en estas conexiones, se simularon con un circuito que facilitaba el seguimiento de las pruebas en el sistema. Este circuito se muestra en la Figura 5.4, el mismo por medio de las terminales NC de un relé tipo C y un interruptor, simulaba la función que cumplen los contactos magnéticos, además contaba con un led verde que formaba parte del lazo de excitación conectado a las terminales del relé, que indicaba cuando la puerta estaba abierta. Se utilizó un transistor como fuente de corriente para cubrir los requerimientos del relé.

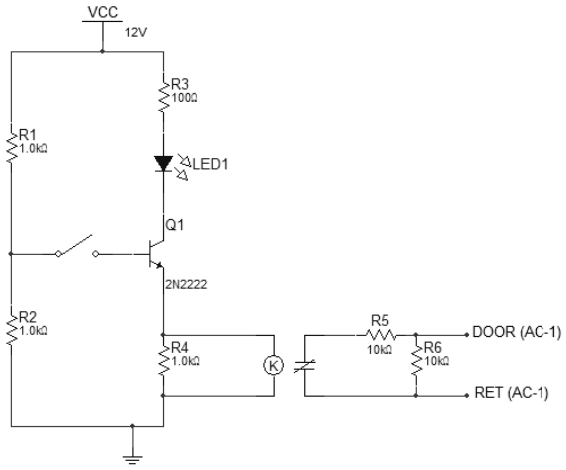



Figura 5.4 Circuito que simula la función de los contactos magnéticos.

La aplicación del control de acceso del bloque Puerta 1 utilizó las dos salidas de las que dispone el AC-1. Al igual que las entradas, cada salida cumplía una función específica, el canal 1 controlaba la cerradura y el canal 2 era una salida auxiliar. Dado que era un módulo de pruebas, la cerradura se simuló colocando un circuito con un led verde, una resistencia limitadora y la fuente de alimentación, en el momento que daba un acceso el sistema activaba la salida, cerrando el circuito y encendiendo el led que indicaba que la cerradura estaba

habilitada. La salida auxiliar se utilizó para la alarma, este circuito estaba conformado por un led rojo y un buzzer (Figura 5.5), que simulaba dispositivos de alarma sonoros y visuales.

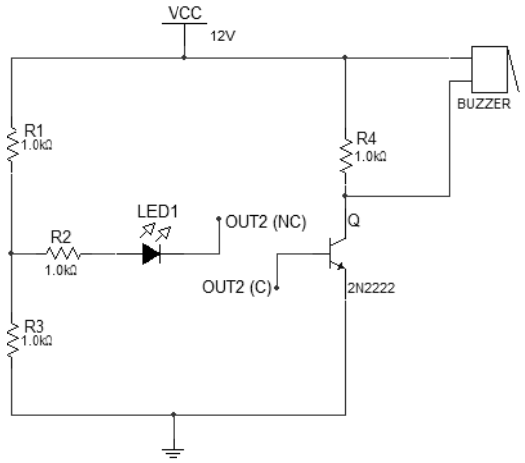



Figura 5.5 Circuito de alarma.

**Bloque Puerta 2**

El bloque Puerta 2 contenía el tercer caso del control de acceso que se probó en el prototipo. El mismo contemplaba la identificación del personal tanto en la entrada como en la salida. Esta conexión se implementó con dos lectores de proximidad de frecuencia de transmisión de 125KHz y protocolo Weigand, para lo que se requirió un AC-1 por cada lector, como se observa en la Figura 5.6.

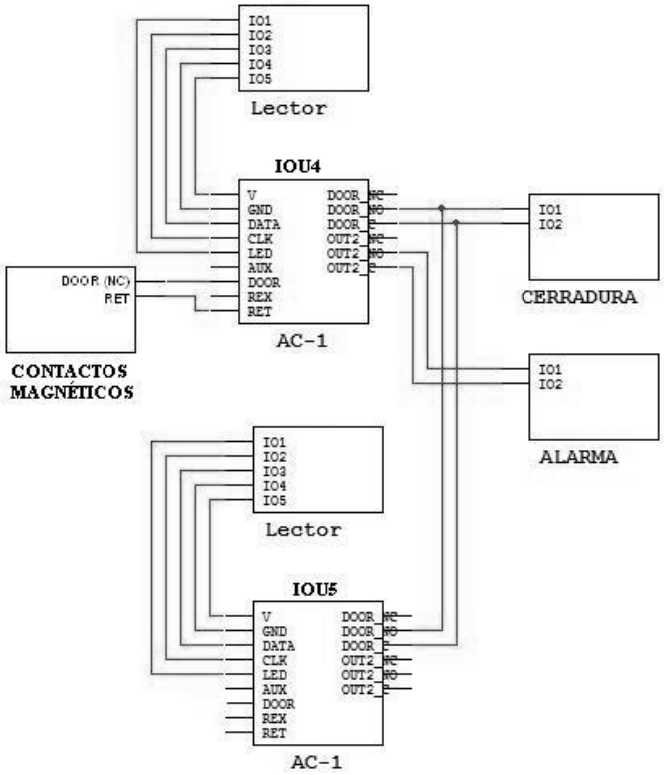



Figura 5.6 Diagrama de conexión de los módulos de la Puerta 2.

En este bloque, al igual que el de Puerta1, se utilizaron los circuitos de prueba para simular el comportamiento de los contactos magnéticos, la cerradura y la alarma. Estos circuitos se conectaron de la misma forma y en los pines correspondientes de acuerdo a su función. En este caso como se utilizaron dos AC-1, es importante notar que el canal 1 de las salidas de ambos debió conectarse a la cerradura para que funcionara correctamente y además el canal 2 de la alarma debía pertenecer al mismo AC-1 en que se conectaron los contactos magnéticos.

Los contactos magnéticos o en este caso el circuito que los simulaba se conectaron en el primer AC-1, únicamente se podían conectar en uno debido al tipo de entradas que monitoreaban la impedancia, por lo que de conectarlos en ambos la impedancia de un AC-1 influiría en el otro afectando la conexión.

**Bloque de entradas y salidas**

El sistema debía integrar el control de acceso y el control de intrusión, los bloques anteriores conformaron la etapa referente al control de acceso, por otra parte este bloque contenía todos los dispositivos que involucraban el desarrollo del control de intrusión, el cual constó de los módulos de entrada DI-8 en los que se conectaron los sensores para el monitoreo y los módulos de salidas DO-4 para las respectivas alarmas de acuerdo a los eventos y las acciones.

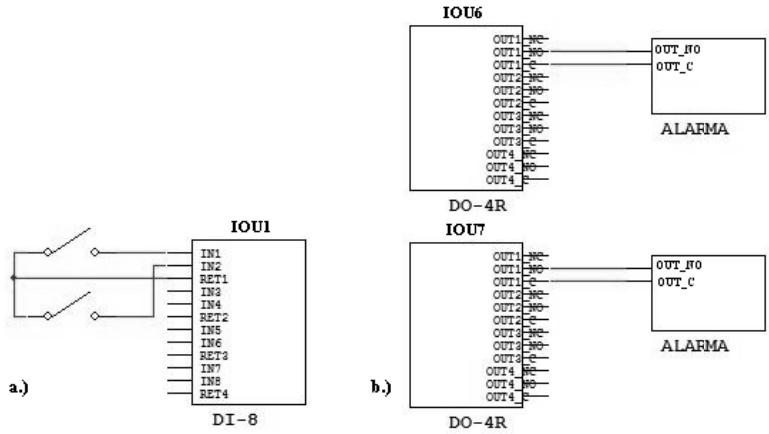



Figura 5.7 a.) Conexión del módulo de entrada. b.) Conexión de los módulos de salida.

El módulo de entradas DI8 detectaba los cambios en las terminales de las entradas monitoreando si el interruptor conectado estaba cerrado (ON) o abierto (OFF), Figura 5.7 a. A estas entradas se conectaron interruptores que permitieron simular el comportamiento de la salida de los sensores.

Las salidas del DO-4R corresponden a relés tipo C de los que se utilizaron los terminales N.O. donde se conectaron los circuitos de alarma que al igual que en el caso de las puertas estaban formados por un buzzer y un led rojo, Figura 5.7 b.

## 5.3. Descripción del software

El sistema de Gestión Andover Continuum era un conjunto de hardware y software. En la descripción del hardware se trataron las diferentes configuraciones en que se utilizaron los dispositivos según los escenarios de prueba y los requisitos del control de acceso y de intrusión, sin embargo el sistema requirió que el controlador y los módulos fueran configurados e ingresados a la red para que interactuaran y ejecutaran las funciones correspondientes. Para esto se tenía el software CyberStation que entablaba la comunicación entre el hardware y la estación de trabajo por el puerto de Ethernet. Por medio de él fue posible configurar el controlador y los módulos, así como crear los programas y las aplicaciones en Plain English para que fueran ejecutadas por el sistema, de esta forma la etapa de software estaba conformada por dos partes, la configuración y el diseño de las rutinas para las aplicaciones.

El software CyberStation estaba basado en los principios de la programación orientada a objetos por lo que cada módulo o controlador configurado, el sistema lo registraba como un objeto y las variables o características relacionadas, formaban parte de los atributos y propiedades de cada objeto.

### Configuración del controlador y los módulos de entrada/salida

#### Objeto Controlador: Configuración del NetController II

El controlador era la parte fundamental del sistema. Por medio de él era posible comunicarse con los módulos, configurarlos y accionarlos. Allí se almacenaban y ejecutaban las aplicaciones del control integral.

La configuración del controlador se realizó en el explorador de CyberStation, ubicando primero la red a la que se quería incluir el controlador y posteriormente presionando click derecho para crearlo seleccionando new *InfinityController* en el menú que se desplegaba, luego aparecía el cuadro de diálogo para editar el

controlador en donde se ingresaba una breve descripción del controlador, el número de identificación del controlador, el modelo, número de serie y la ruta en donde estaba ubicado.

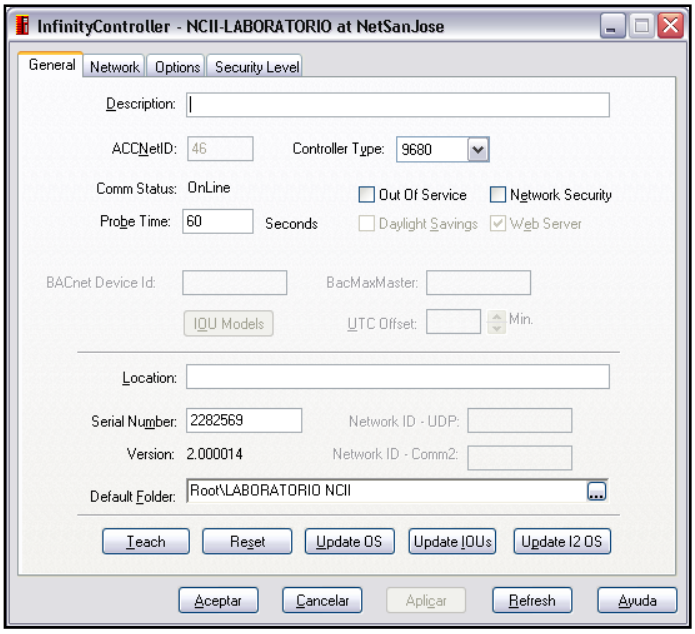
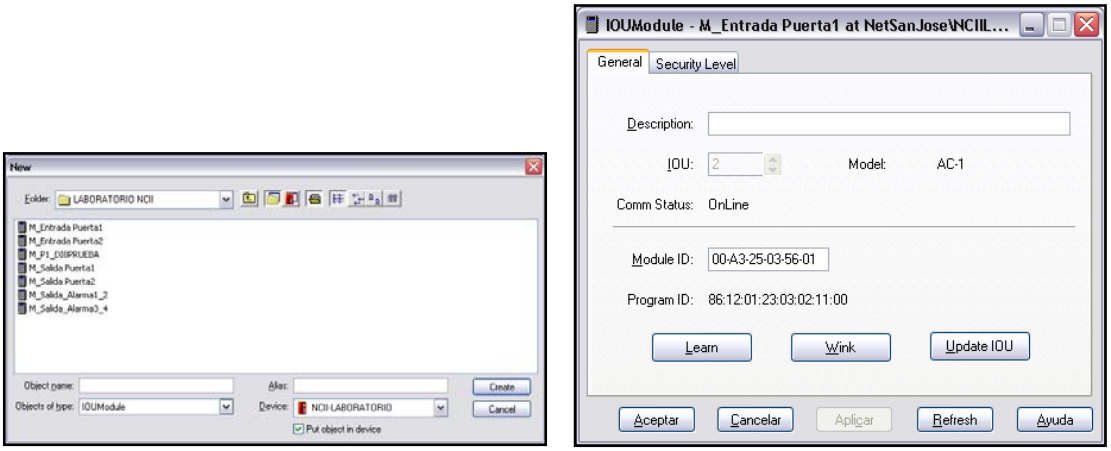



Figura 5.8 Cuadro de configuración del controlador.

### Objetos módulos de entrada/salida: AC-1, DI-8 y DO-4

El módulo se creó dentro de la carpeta que pertenecía al controlador previamente configurado, al presionar el click derecho y seleccionar *new IOU Module*, posteriormente se desplegó un cuadro de diálogo por medio del cual se realizaba la configuración. Se presionaba el botón *commission*, que poseían todos los módulos, con lo que se enviaba la información de identificación a la estación de trabajo, que la recibía al dar click en *learn* en el cuadro de dialogo, además se le otorgaba el número de módulo correspondiente de acuerdo a los que estaban conectados, cabe mencionar que el máximo era de 32 módulos por cada controlador.




a.) b.)

Figura 5.9 Cuadro de diálogo para a.) creación del módulo, b.) configuración del módulo.

### Objetos Áreas

Una vez que se tuvieron los módulos dentro de la red, se procedió con la creación de las áreas con las que se ligarían los módulos correspondientes al control de acceso. Al igual que para los módulos las áreas se crearon dentro de la carpeta del controlador correspondiente presionando click derecho y seleccionando *new area*, apareciendo luego un cuadro de diálogo en el que se describió el área y se agregaron las puertas relacionadas al área y al dar click en aplicar quedó creada.


Figura 5.10 Cuadro de configuración de área.

### Objetos Puertas

La configuración de las puertas era una parte esencial en el desarrollo del control de acceso. Para crear el objeto puerta se siguió el mismo procedimiento que en los dos objetos anteriores, ubicándose en la carpeta del controlador, presionando click derecho y seleccionando new door, accesando de esta forma al cuadro de diálogo para la configuración.

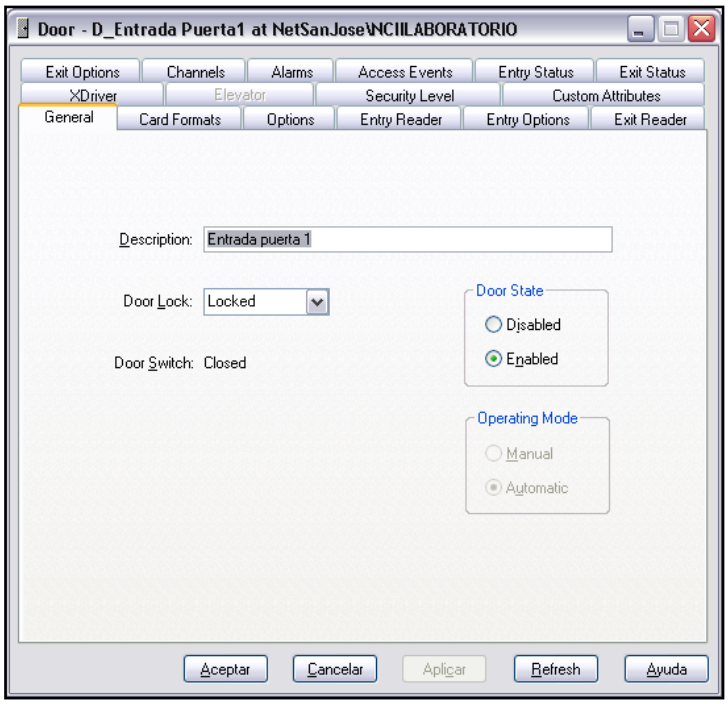



Figura 5.11 Cuadro de configuración de puerta.

El primer paso en la configuración fue habilitar la puerta dentro del sistema y bloquearla, luego de esto se procedió con la configuración de los canales del AC-1 de acuerdo a la conexión realizada, así como los lectores y las alarmas.

Cada canal del AC-1 en sí mismo estaba previsto para una función específica. Según la conexión y los pines utilizados se definió la configuración con la que iba a ser reconocido por el sistema.

La salida de la puerta, en donde se conectaron las terminales de la cerradura correspondió al canal uno, adicionalmente se configuró el tiempo en segundos durante el cual se enviaba la señal que habilitaba la cerradura y también el tiempo en segundos antes de que se diera el evento de puerta abierta que activaba la alarma. El canal dos de las salidas se seleccionó para la alarma, asignándole la duración en segundos, es decir el periodo en que el relé cambiaba su estado, así como los segundos de espera antes de que se diera un evento de puerta forzada.

En cuanto a las entradas, el canal dos se utilizó para las conexiones de los contactos magnéticos y el canal tres para la entrada de solicitud de salida, que se utilizó en la Puerta 1 tanto para el sensor como para el interruptor, motivo por el cual se utilizaron dos AC-1, fue necesario en este caso habilitar esta función en la opción “desbloquear con solicitud de salida”. En ambos canales se debió indicar el tipo de conexión que se había utilizado que como se dijo anteriormente era NCSerie-Paralelo.

Los lectores también debieron ser configurados. Dentro de cada puerta venía indicado el lector de entrada y el lector de salida, sin embargo solo se configuraba uno de los dos por cada AC-1, en cualquier caso el proceso fue el mismo, se debió indicar el número de módulo en el que se conectó el lector, según el asignado cuando se crearon los objetos módulos de entrada/salida, así como el canal uno. Una parte importante era asignar el área, previamente creada, con la que se iba a ligar la puerta y seleccionar el método de la validación del acceso, por tarjeta de identificación en esta aplicación.

Las alarmas relacionadas a cada puerta se seleccionaban en el espacio destinado a esto del cuadro de diálogo. Las mismas debieron ser creadas previamente mediante registros y notificaciones de la manera que se describe más adelante en este capítulo. Para agregarlas se buscaba la ruta en donde se encontraba el registro de la alarma y se habilitaba. Algunas de estas alarmas

eran activadas por variables numéricas y no por atributos del objeto por lo que debían indicarse como puntos de alarma dentro de la configuración para que fueran reconocidas como tales.

Adicionalmente desde el explorador era posible ingresar al cuadro de edición en cualquier momento, para realizar modificaciones o bien observar los eventos relacionados con la puerta, ya que de dentro de el existía un espacio en donde quedaban registrados llamado *AccessEvents*.

**Registros de alarmas y notificaciones**

Las alarmas se configuraron como registros que se crearon de la misma manera que los objetos anteriores. Debieron ubicarse dentro de la misma carpeta del controlador. Cada registro se creó seleccionando *new AlarmEnrollment* y configurándolo en el cuadro de diálogo respectivo.

En el cuadro de diálogo se incluyó para cada alarma la notificación que se utilizaría en caso de que la alarma fuera activada, esta notificación se conocía como *EventNotification* y debió ser configurada previamente. Además, se indicaba cual variable o atributo accionaba la alarma y el tipo de alarma, especificando la condición para la activación en el espacio *Algorithms,* finalmente en *Feedback* se podían agregar los mensajes de aviso que aparecerían en la barra de alarmas de CyberStation al darse la alarma.

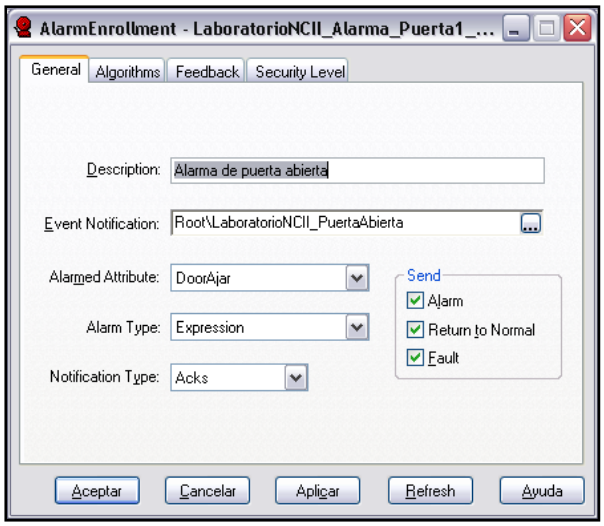



Figura 5.12 Cuadro de configuración del registro de alarma.

Los EventNotification permitieron configurar el tipo de mensajes o acciones que se llevaban a cabo durante la activación de la alarma. Los objetos de notificación se creaban de la misma manera que en los casos anteriores.

Una vez que se ingresaba al cuadro de edición se incluía una breve descripción, la prioridad si se requería y las repeticiones. Además se podían asignar diferentes colores o letras según la alarma que permitieran indicar los niveles de importancia. En el espacio *Actions* se presentaba una lista de acciones en donde se elegían las que utilizaban para cada alarma, estas acciones ocurrían en la estación de trabajo y consistían en el envío de mensajes a través del panel de alarma que aparecía en la pantalla principal de CyberStation o sonidos, entre otros.

Dentro del cuadro de diálogo en *Delivery* se debían incluir las estaciones de trabajo hacia las cuales debían ser enviadas las notificaciones y en *Deactivate* se seleccionaban las acciones que deshabilitaban la alarma o la retornaban a la normalidad.

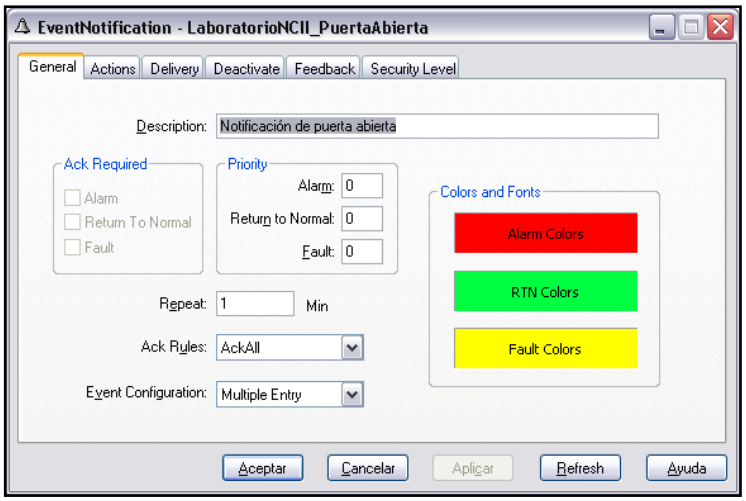
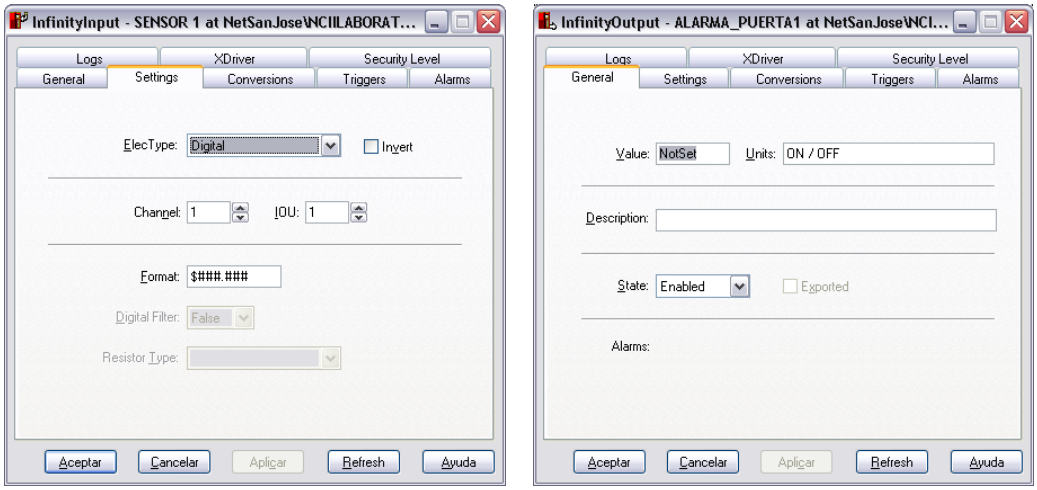



Figura 5.13 cuadro de configuración de notificaciones de alarma.

### Objetos entrada y salida

Las entradas y las salidas de los módulos DI-8 y DO-4 se debieron configurar cada una de forma individual. Para crearlas se ubicó la carpeta del controlador y allí se seleccionó en el menú, ya fuera *InfinityOutput* o *InfinityInput*. En el cuadro de edición se habilitaban, se identificaba el tipo entrada o salida, digitales en este caso, así como el canal y el número del módulo al que pertenecían. Estas entradas y salidas podían ser manipuladas o modificadas directamente por medio de los programas en PlainEnglish.




a.) b)

Figura 5.14 cuadro de configuración de: a.) entradas y b.) salidas.

## Rutinas y aplicaciones de control

La siguiente etapa del software del sistema integral de seguridad involucró las rutinas por medio de las cuales se manejó la interacción entre los dispositivos y el control general. Se crearon las rutinas para el control de acceso y el control intrusión, así como las variables y condiciones que establecieron la relación entre ellas que finalmente produjeron un sistema unificado.

Las variables numéricas utilizadas dentro de las rutinas debieron ser configuradas de forma similar a los módulos de hardware. Estas variables se reconocían como *InfinityNumeric* y se editaban en el cuadro de diálogo. Las mismas eran reconocidas por sus alias en los programas de Plain English.

La figura 5.16 muestra el cuadro de diálogo y en este se debieron especificar las unidades y una breve descripción. La variable se habilitó desde aquí y cada vez que fuera necesario era posible observar el valor de la misma en esta

ventana. Al igual que las entradas y salidas a esta variable era posible asignarle una alarma por medio del cuadro de configuración.

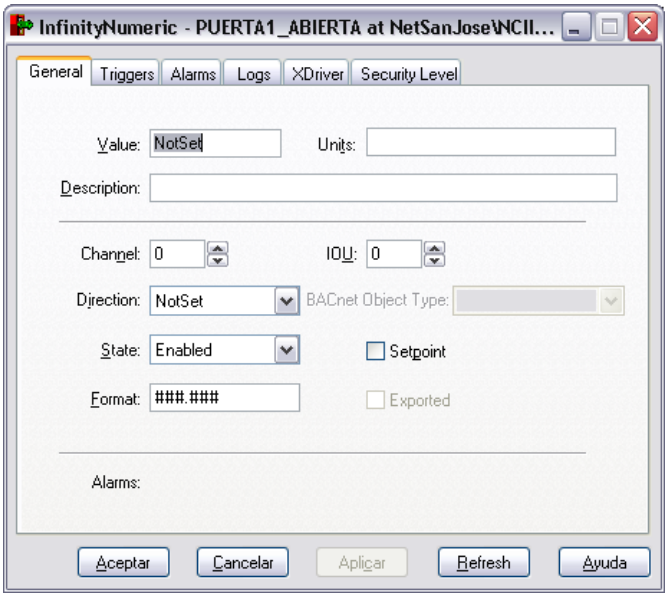



Figura 5.15 Cuadro de configuración de variables numéricas.

**Rutina de conteo para la Puerta 1 y Puerta 2**

Esta rutina fue la encargada de registrar el conteo de las personas que entraban y salían de un área específica, la cual se delimitaba a partir del sistema de control de acceso. Adicionalmente, el sistema debía ser capaz de discernir entre un acceso válido sin ingreso y otro con ingreso, ya que era determinante en el reconocimiento de los eventos que eran tomados en cuenta para el conteo.

La rutina estaba dividida en cuatro bloques, el primero de ellos se encargaba de registrar el ingreso de las personas, el segundo la salida, el tercero de los bloques desactivaba las alarmas y el cuarto monitoreaba la inactividad. Para el desarrollo de la rutina era necesario interactuar con los atributos de los objetos de puerta por medio de los cuales fue posible identificar los eventos.

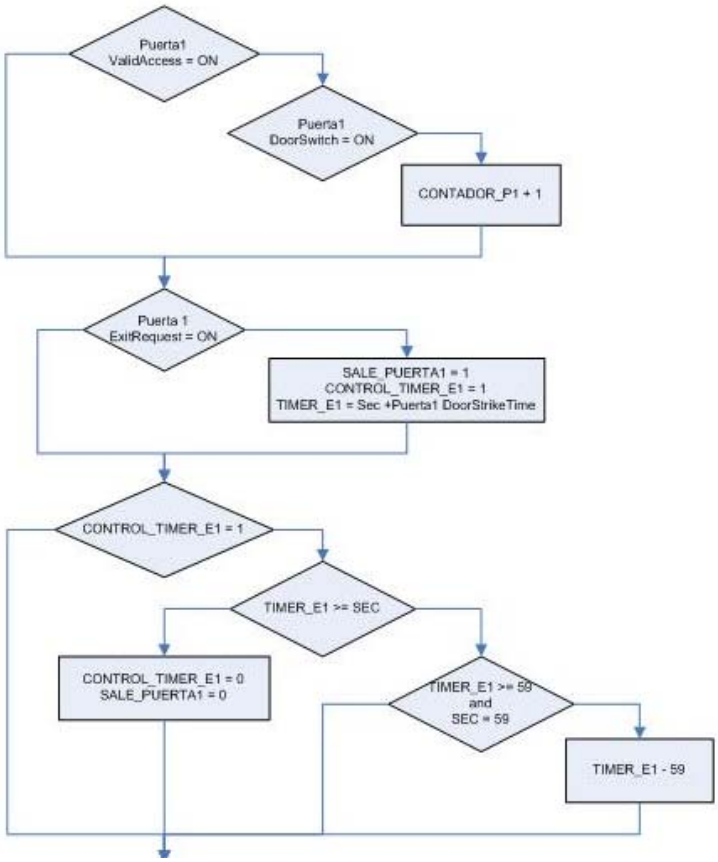



Figura 5.16 Diagrama de flujo de la rutina de conteo de la Puerta1

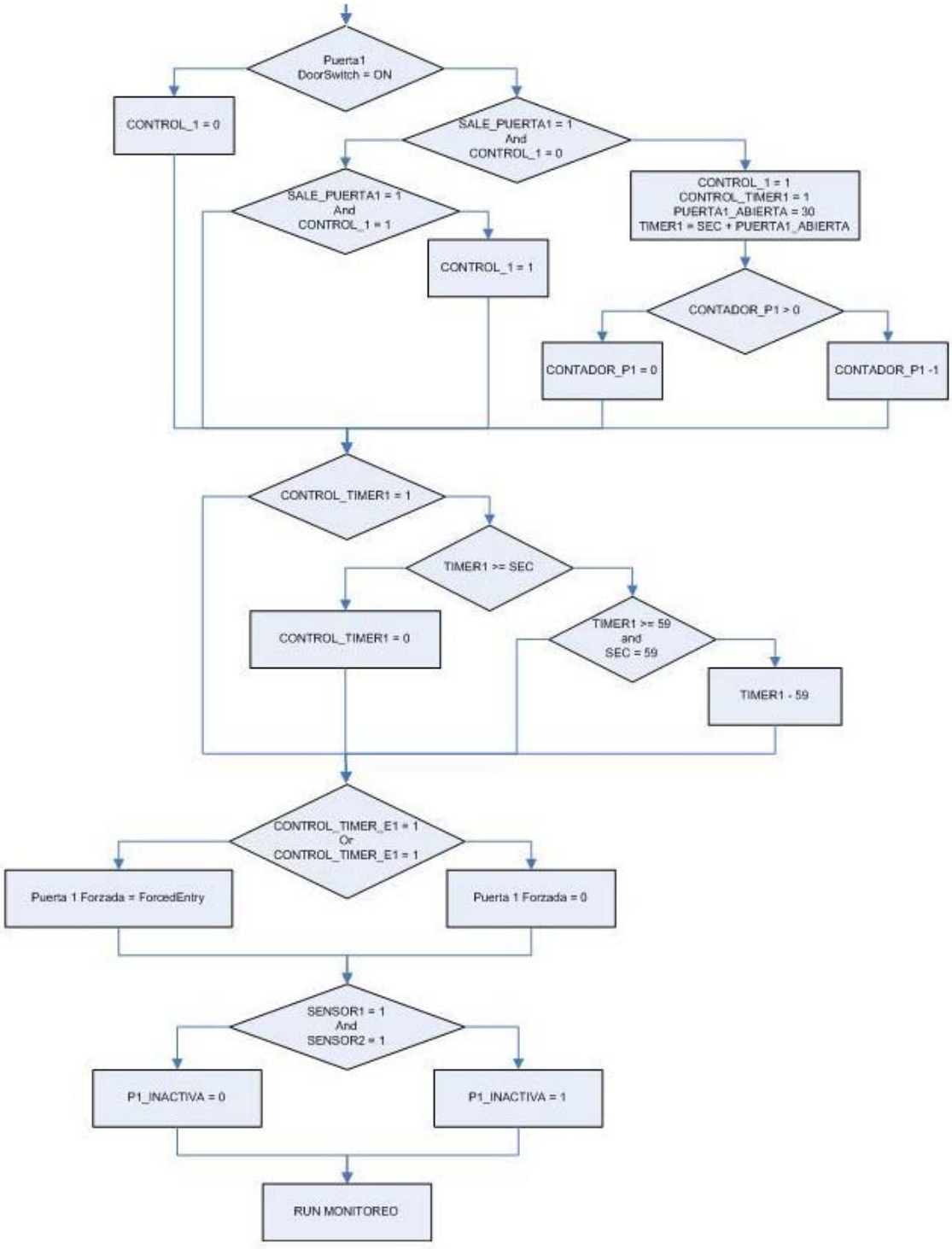



Figura 5.17 Diagrama de flujo de la rutina de conteo de la Puerta1 (Continuación).

En el bloque de ingreso, cuando el sistema registraba un acceso válido a través de la señal de ValidAccess y siempre que se detectaba la apertura de la puerta DoorSwitch, ésta acción quedaba registrada como un ingreso por lo que la variable numérica del contador aumentaba en uno. Esto demandaba que cada persona debía obligatoriamente registrarse al entrar, estableciéndose como una de las políticas de seguridad.

El segundo bloque encargado del registro de salidas era el que marcaba la principal diferencia entre la rutina para la puerta 1 y la puerta 2. Esta diferencia dependía de la configuración y la conexión de los dispositivos de salida utilizados.

La Puerta 1, como se ha mencionado antes, poseía una configuración de salida en que se utilizaba un interruptor y un sensor de movimiento como dispositivos de solicitud. En ambos casos la señal de entrada que indicaba la solicitud, que llegaba al sistema a través del AC-1, tenía una duración mayor a un ciclo del reloj por lo que era leída varias veces por el sistema, lo que obligó la utilización de una secuencia de un detector de flanco que permitiera registrarlo únicamente en el momento en que se diera el cambio en la señal.

Inicialmente la rutina monitoreaba tanto la entrada que pertenecía al interruptor como en la que estaba conectado el sensor, al detectarse un cambio en el atributo ExitRequest se modificaba el estado de la variable SALE_PUERTA1, lo que indicaba la existencia de la solicitud, de igual forma se inicializaba un temporizador que determinaba la duración de la solicitud por un tiempo igual a la señal que habilitaba la cerradura, especificado en el cuadro de configuración de la puerta, de esta manera era posible equiparar ambos tiempos lo que permitía contabilizar la salida en el momento en que se diera una apertura de la puerta durante ese rango de tiempo. La apertura de la puerta era indicada por el cambio en DoorSwitch, lo cual ejecutaba una secuencia de un detector de flanco para evitar que la señal de solicitud se contabilizara varias veces, por

medio de una variable de control CONTROL_1, hasta que la variable de solicitud volviera a su estado inicial cero. Con esto quedaba registrada la salida en la variable CONTADOR_P1, disminuyéndolo en uno o en el caso de que fuera cero se mantenía igual. En este punto también se activaba el temporizador que desactivaba la alarma de puerta forzada durante el tiempo en que la puerta se mantuviera abierta.

La Puerta 2 tenía conectado en la salida otro lector que permitía identificar a la persona en la salida, en este caso el sistema era más confiable ya que cada persona que salía debía pasar su tarjeta por el lector garantizando que todos iban a estar incluidos en el conteo, no así en el caso de la Puerta 1.

Al igual que en la Puerta 1 se monitoreaba la ocurrencia de un evento que solicitara habilitar la cerradura, esto se hacía por medio de ValidAccess ya que era un lector, al detectarse esta señal se activaba la variable SALE_PUERTA2 que mantenía la solicitud activa por medio de un temporizador cuya duración dependía del tiempo en que estuviera habilitada la cerradura, DoorStrikeTime. Luego de esto se monitoreaba la posible apertura de la puerta, la cual indicaría que ocurrió una salida válida, con esto se retornaba SALE_PUERTA2 a su valor inicial, se disminuía en uno la variable CONTADOR_P2 e iniciaba el temporizador para deshabilitar la alarma forzada durante la apertura de la puerta.

Como se ha mencionado en ambos casos del bloque de salida, la alarma de puerta forzada debió ser desactivada ya que el sistema no podía identificar la salida como válida, esta función la cumplía el bloque para desactivar la alarma. El evento ExitRequest no la validaba, lo que impedía que el sistema ignorara la acción de apertura forzada, motivo por el cual se requirió de una rutina que la desactivara. De igual forma para el caso de la Puerta 2, aunque la acción estaba dada por medio de un lector y existe un ValidAccess, al no existir una conexión con los contactos magnéticos, el sistema no lo reconocía y enviaba una señal de ForcedEntry por lo que también debió que ser desactivada.

La rutina que desactivaba la alarma consistió en dos temporizadores, ambos eran activados dentro del proceso del conteo de salida. El primer temporizador se iniciaba en el momento en que existiera un ExitRequest o solicitud de salida, cuya duración dependía del tiempo en que se enviaba la señal que habilitaba la cerradura, lo que garantizaba que mientras existiese una solicitud de salida la alarma estaría desactivada, el segundo temporizador era activo únicamente si se concretaba la salida, es decir al registrarse la apertura de la puerta. Para activar y desactivar la alarma se monitoreaban las variables que controlaban ambos temporizadores si una o ambas variables eran activas se desactivaba la alarma cambiando el estado de la variable PUERTA1_FORZADA a cero y cuando se reactivaban se asignaba a PUERTA1_FORZADA el valor del atributo ForcedEntry.

El último bloque de esta rutina se encargaba de monitorear las entradas en las que se encontraban conectados los sensores, de esta forma era posible conocer si había actividad en un área determinada.

**Rutina de monitoreo de la Puerta1 y Puerta2**

La rutina de monitoreo era la encargada de relacionar las funciones del control de acceso con el control de intrusión, monitoreando los cambios y el estado de los contadores en los puntos de acceso, así como los sensores relacionados a esa área específica. Por medio de esta rutina era posible activar o desactivar las alarmas de intrusión.

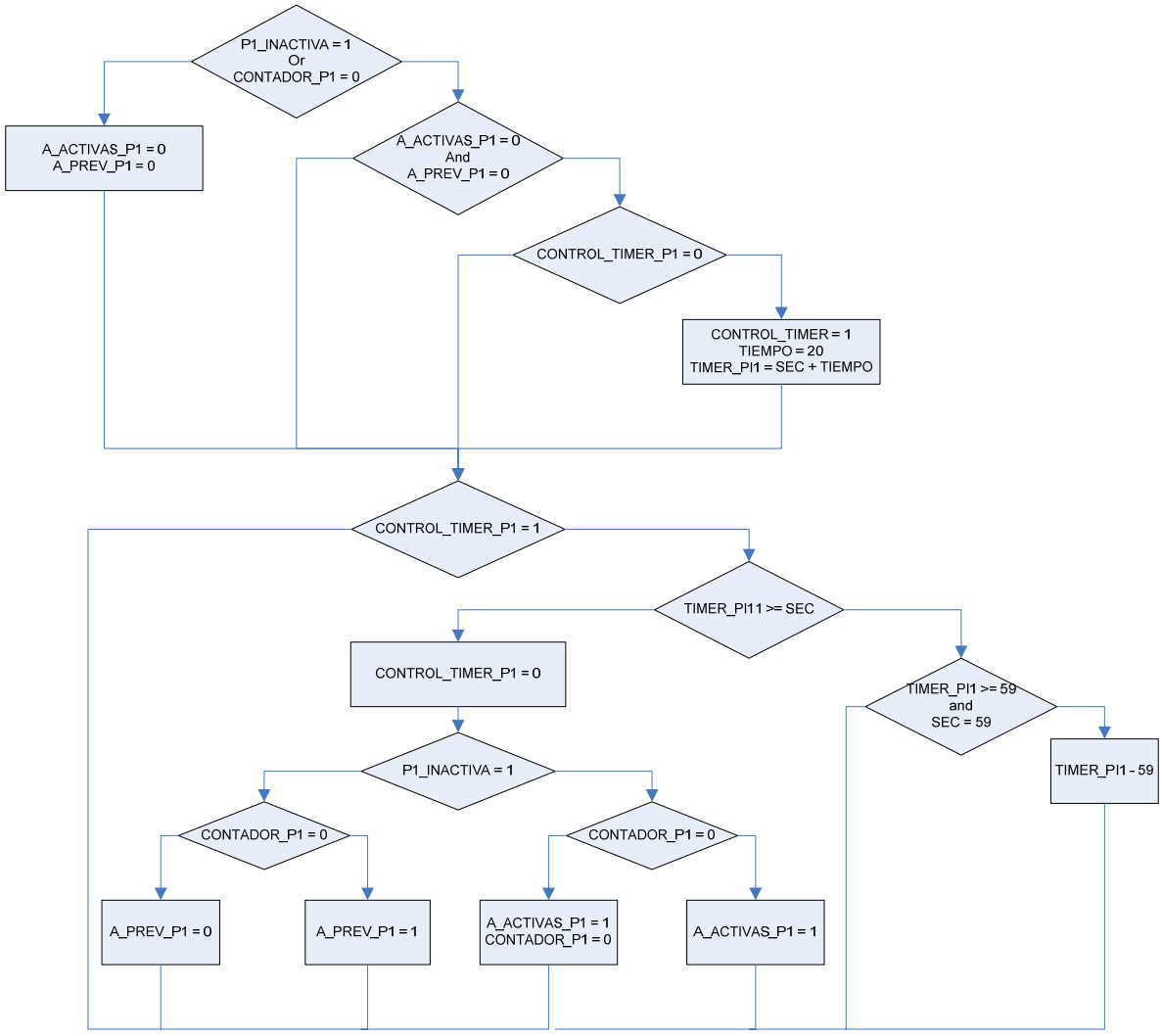



Figura 5.18 Diagrama de flujo de la rutina de monitoreo de la Puerta1.

Existían dos condiciones para que se realizara el monitoreo, las cuales dependían de variables que eran modificadas durante la ejecución de la rutina de conteo de ingreso y salida, CONTADOR_P1 y P1_INACTIVA. Si el contador marcaba cero o bien en el área no se detectaba actividad se iniciaba la secuencia de monitoreo.

El primer paso era verificar el estado de las alarmas tanto la de intrusión como la de prevención, si eran inactivas se iniciaba la secuencia de activación con el temporizador, cuyo tiempo límite era modificable y se almacenaba en la variable

TIEMPO. Este temporizador daría una ventana de tiempo antes de que se decidiera si se requería activar o no las alarmas, esto para brindar el tiempo suficiente para que el personal pudiera salir del área.

Una vez concluido el tiempo del temporizador se analizaba la inactividad, de aquí se desprendían dos casos. El primer caso, si existía inactividad en el área se activaban las alarmas (A_ACTIVAS_P1 =1) y el contador se retornaba a cero, esto para prevenir que alguna persona hubiera salido del área sin registrarse por el lector y por lo tanto continuaba contabilizado por el sistema. El segundo caso contemplaba la permanencia de personas dentro del área con los sensores indicando actividad, de ser así, se verificaba el contador, si el contador era diferente de cero las alarmas permanecían inactivas, por el contrario si el contador indicaba cero se activaba una alarma preventiva que indicaba que alguna persona permanecía dentro del área sin estar registrada por el contador.

**Rutina de alarmas**

La rutina de monitoreo modificaba la variable A_ACTIVAS_P1, la cual era la condición principal para la ejecución de la rutina de alarmas. Si las alarmas se encontraban activas se procedía con el muestreo continuo de los sensores si en algún momento se detectaba movimiento, se activaban los temporizadores que regulaban el sonido de las alarmas.

Adicionalmente cada alarma al ser accionada enviaba una notificación a la estación de trabajo por medio de una variable que estaba ligada a un registro de alarma.

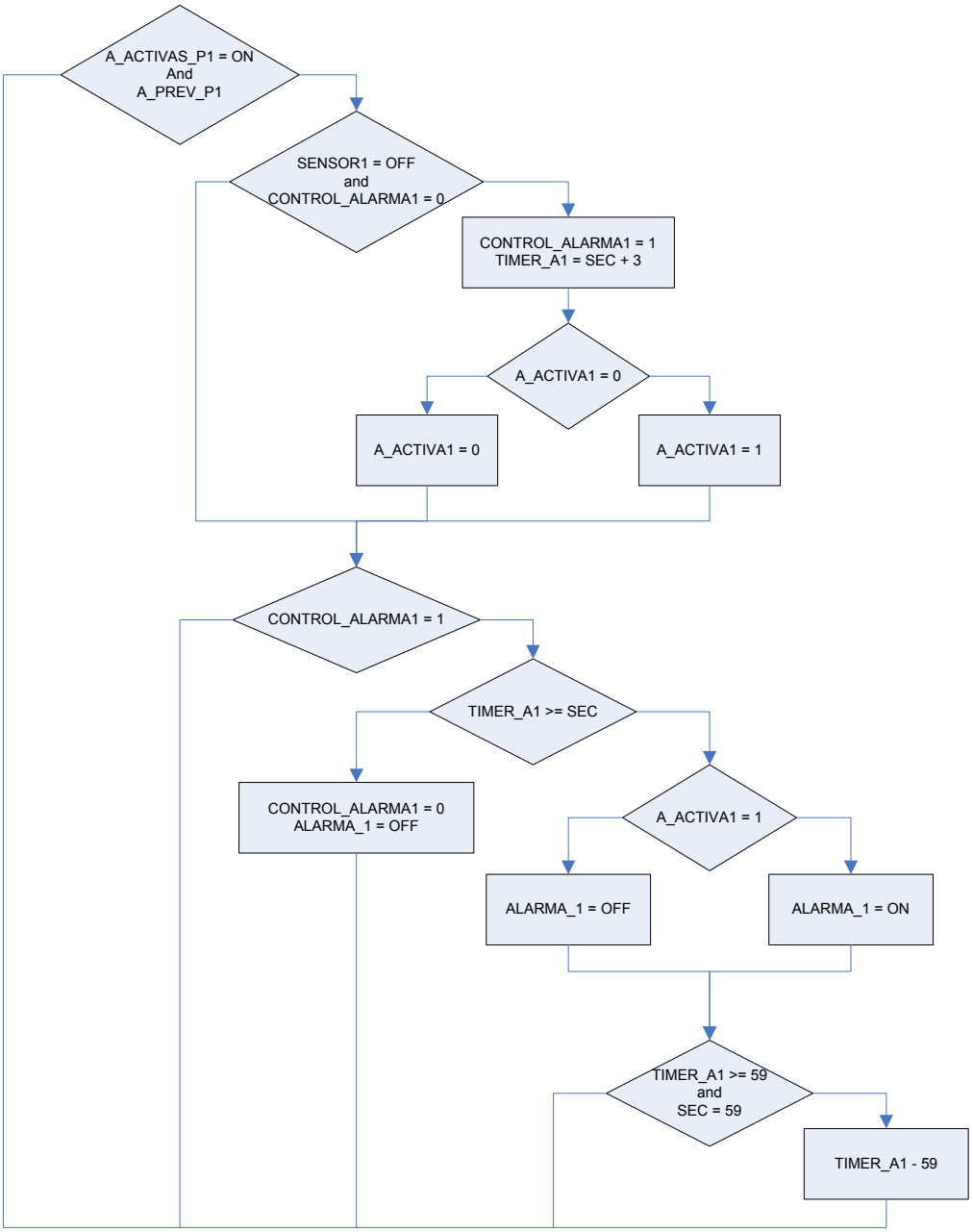



Figura 5.19 Diagrama de flujo de la rutina de alarmas de la Puerta1. (Esta rutina es solamente para el sensor 1, las demás funcionan de la misma forma.)

# Capítulo 6. Análisis de Resultados

La elaboración del prototipo implicó tanto el desarrollo a nivel de hardware como software y la interacción entre estos. El primer paso consistió en el diseño del módulo de pruebas, de manera que incluyó todas las posibles conexiones en que se podía utilizar el sistema. El segundo paso involucró la interacción con los dispositivos a nivel de software y el diseño de las aplicaciones. Este paso se podría decir que se dividió en dos etapas, en la primera de ellas se configuraron los dispositivos para el control de acceso y se realizaron las pruebas para evaluar la funcionalidad de estos; en la segunda etapa se buscaron las soluciones a los problemas y deficiencias encontradas en la etapa anterior, para finalmente interrelacionar los dispositivos del control de acceso y el control de intrusión.

El diseño del módulo de pruebas requirió de la interconexión de diferentes dispositivos para obtener un control integral de acceso e intrusión. Para esto fue necesario analizar las características eléctricas de cada uno de ellos, lo que se muestra en la **Tabla 6.1**, así como conocer su funcionamiento de manera que fuera posible determinar la compatibilidad entre ellos.

**Tabla 6.1** Parámetros eléctricos de los componentes del sistema integral de seguridad

| **Dispositivo** | | **Características** |
|---|---|---|
| Fuente | | 120/240 $V_{AC}$ 50W 24$V_{DC}$ |
| Controlador NetController II 9940 | Fuente-Controlador | 24$V_{AC}$ @ 50/60Hz<br>12-28 $V_{DC}$<br>10W |
| Módulos AC-1 | Módulo-Fuente | 24 $V_{DC}$ máximo.<br>2.6W + consumo del lector |
| | Módulo-Controlador | RS-485 Distancia máxima 610m |
| | Módulo-Lector | Alimentación seleccionable<br>5V @ 120mA o 12V @ 180mA<br>2 entradas data0, data1<br>1 salida led |
| | Entradas del módulo | 3 supervisadas, R=10KΩ<br>NCserie, NOserie, NCparalelo,<br>NOparalelo, NCSerie-Paralelo,<br>NOSerie-Paralelo |
| | Salidas del módulo | 2 relé tipo C 5A @ 24$V_{DC-AC}$ |
| Módulos DI-8 | Módulo-Fuente | 10-28 $V_{DC}$<br>0.8W |
| | Módulo-Controlador | RS-485 Distancia máxima 610m |
| | Entradas del Módulo | Contacto cerrado o 0-5V<br>Impedancia de entrada 10KΩ<br>Ancho de pulso mínimo 50ms<br>0.5 mA máximo. |
| Módulos DO-4R | Módulo-Fuente | 10-28 $V_{DC}$<br>2.8W |
| | Módulo-Controlador | RS-485 Distancia máxima 610m |
| | Salidas del módulo | 4 relé tipo C<br>240 $V_{AC}$ @ 5A<br>30$V_{DC}$ @ 5A |
| Lector de proximidad | | 5 a 16$V_{DC}$<br>0.45W<br>Protocolo Wiegand<br>Frecuencia de transmisión 125KHz.<br>Frecuencia de excitación 125KHz |
| Sensores de solicitud de salida RTE1000 | | 12 o 24 $V_{DC}$ seleccionable<br>7mA<br>Salida relé tipo C 30$V_{CD}$ @ 1A<br>Patrón de detección 2.6mx1.5m<br>Altura 2.3m |
| Sensores de movimiento RX-40PT | | 9.5 a 16V<br>8mA<br>Salida relé N.C. 28$V_{DC}$ @ 0.2A<br>Patrón de detección 12mx12m<br>Altura 2.4m |
| Luz estroboscópica | | 12 o 24 $V_{CD}$ |

Según la tabla mostrada fue posible observar que la fuente utilizada por el controlador superaba en 40W la potencia requerida por este dispositivo, lo que brindó la posibilidad de utilizarla para la alimentación de los módulos enlazados a él, de esta forma la alimentación para los módulos fue suplida por la misma fuente a través del controlador, ya que este proveía el conector con 2 líneas adicionales de alimentación que venían de la fuente de 24V. Cabe mencionar que esto no fue un requisito, de haber sido necesario se pudieron utilizar fuentes adicionales siempre y cuando cumplieran con los requerimientos de tensión y corriente. En este caso se facilitó por la cercanía de los dispositivos, sin embargo de acuerdo a las características del controlador y el protocolo de comunicación RS-485, si el diseño del sistema lo ameritaba la conexión pudo realizarse a una distancia máxima de 610m del módulo hacia el controlador.

El controlador utilizó el protocolo RS-485 para la comunicación con los módulos de entrada y salida, de acuerdo a este protocolo el controlador era capaz de manejar 32 módulos, de los cuales se utilizaron siete en el diseño del prototipo, cuatro AC-1 para los controles de acceso, un DI-8 para las entradas y dos DO-4 para las salidas, en el control de intrusión.

Los módulos AC-1 tenían un consumo de 2.6W y los lectores conectados en ellos de 0.45W en total el consumo demandado por los módulos AC-1 y los lectores para las conexiones de las puertas fue de 11.75W. Estos módulos además de permitir el acceso por medio de los lectores proveían los pines para la conexión de los dispositivos adicionales que monitoreaban el comportamiento de la puerta como los contactos magnéticos y de ser necesario, para los dispositivos de salida como sensores o interruptores.

Un punto importante al utilizar los AC-1 fue la configuración de las resistencias utilizadas en las entradas, las cuales independientemente del circuito de entrada seleccionado, debieron ser todas de 10KΩ, ya que el AC-1 monitoreaba la impedancia de entrada para determinar el estado del interruptor.

En la Tabla 3.1 se mostró el comportamiento de las diferentes configuraciones, de estas se utilizó la configuración Serie-Paralelo N.O. o N.C. según fue necesario, debido a que presentaba la ventaja de reconocer únicamente dos estados válidos ON/OFF y en el caso de un corto circuito o por el contrario circuito abierto el sistema lo reconocía como un estado indefinido.

El prototipo que se observa en la Figura 6.1, buscaba ejemplificar en un solo módulo las diferentes conexiones y configuraciones en que se podían utilizar los dispositivos. Para realizar las pruebas fue necesario utilizar circuitos de prueba que simularan algunas de las condiciones y así evaluar la respuesta, el comportamiento y la interacción entre los dispositivos, el controlador y el software, es decir las aplicaciones.

Figura 6.1 Módulo de pruebas del sistema integral de seguridad.

Los circuitos de pruebas incluyeron luces indicadoras y sonidos que permitieron reconocer los estados tanto en las entradas como en las salidas e incluso observar la duración de los mismos, y así calcular los tiempos adecuados para las diversas acciones como las señales que habilitaban las cerraduras, o bien el tiempo de espera antes de la activación de una alarma, así como la ejecución de las alarmas y así reconocer y evaluar la secuencia de la aplicación dentro del procedimiento que se estaba probando. Entre los circuitos de simulación se tenían el circuito de los contactos magnéticos, el de alarma y el de cerradura, además de los utilizados para simular los sensores de movimiento, como se muestran en la imagen de la Figura 6.2.


Figura 6.2 Circuito de prueba para la Puerta 2.

Los contactos magnéticos eran parte fundamental en el funcionamiento del sistema del control de acceso, permitieron conocer si la puerta fue abierta, los mismos funcionaban como un interruptor conectado en las entradas de los pines 7 y 9 del AC-1. Estos se utilizaban en la implementación real del sistema, sin embargo al ser un circuito de pruebas se utilizó un relé para cumplir con la función de los contactos magnéticos, de manera tal que funcionara como un interruptor aislado permitiendo que el circuito que accionaba el relé incluyera una luz indicadora del estado del mismo, facilitando el reconocimiento de la acción de la puerta, ya fuera abierta (led encendido) o cerrada (led apagado).

Las salidas de los AC-1 correspondieron a relés de 5A @ 24V que cerraron los circuitos de alimentación de la cerradura o los dispositivos de alarma, ya fuera sonora, visual o ambas. En ambos casos se utilizaron circuitos que simularon la ejecución de ambas acciones. Para la cerradura se utilizó un led verde, esto permitió observar el tiempo durante el cual la cerradura permanecía habilitada y para la alarma se utilizó un circuito con un buzzer y un led rojo que se accionaba de acuerdo a la configuración de la alarma.

Los módulos de entrada y salida, DI-8 y DO-4, en conjunto tuvieron un consumo de 6.4W. Al igual que los AC-1 la alimentación para estos módulos fue de 24V tomado de la fuente que alimentaba al controlador. Los sensores de movimiento RX-40PT utilizados en el sistema, poseían una salida correspondiente a un relé tipo C. En el módulo de pruebas, para una mayor facilidad a la hora de realizar las evaluaciones, se utilizó únicamente un sensor conectado al DI-8 y en las siete entradas restantes se conectaron interruptores para simular el comportamiento de los sensores. En cuanto a los módulos DO-4, las salidas de estos se conectaron a circuitos que simulaban alarmas.

Los módulos conectados no interactuaron por sí mismos, sino que debieron ser configurados para que fueran reconocidos por el sistema. El software CyberStation fue el encargado de establecer la comunicación, el monitoreo y control de la plataforma. Los controladores y los módulos se identificaron y configuraron a través de este software. El hecho de que CyberStation fuera un software basado en los principios de la programación orientada a objetos, facilitó la comprensión e interacción con los diferentes módulos, debido a que cada uno de ellos fue configurado como un objeto independiente, con un conjunto de atributos y propiedades, que pudieron ser manipuladas y modificadas a través de los programas o aplicaciones creadas en el lenguaje de programación Plain English.

La configuración de los módulos de entrada y salida, DI-8 y DO-4 respectivamente, se realizó ingresando al sistema cada una de sus entradas y salidas de forma independiente, estas pudieron ser manipuladas como variables de entrada y salida dentro de un programa en Plain English, lo que brindó versatilidad al sistema al poder interactuar directamente y disponer de ellas de acuerdo a las necesidades de la aplicación. Adicionalmente un módulo AC-1 permitió ser configurado no solo como parte de un control de acceso, sino que también como un módulo de entradas y salidas de manera similar a los DI-8 y DO-4.

El principio fundamental en el desarrollo de este sistema se centró en la integración del control de acceso y el control de intrusión, es decir, la comunicación e interacción entre estos. En los párrafos anteriores se analizó la conformación del sistema a nivel de hardware, conociendo principalmente los módulos utilizados y los circuitos de prueba. Además se mencionó la existencia del software que permitió la configuración, programación e interacción. Para analizar de cerca las funciones del sistema como un prototipo era mejor segmentarlo de acuerdo a sus partes funcionales, se trató de esta manera un control de acceso con tres posibles casos y un control de intrusión con 8 entradas y salidas.

En los dos primeros casos del control de acceso se tomó como base la conexión utilizada para ingresos en donde existió identificación únicamente en la entrada, valiéndose de un interruptor en el primer caso y un sensor de solicitud de salida en el segundo caso, figura 6.3. Esta conexión requirió de un módulo AC-1 para su funcionamiento, y la configuración que especificara la utilización de los dispositivos de salida. El tercero utilizaba dos AC-1, necesarios para lograr la identificación tanto en la entrada como en la salida, figura 6.4, lo cual fue el objetivo de esta última conexión.


Figura 6.3 Configuración de Puerta con lector en la entrada y dispositivo de salida. (Interruptor y sensor REX)


Figura 6.4 Configuración de Puerta con lector en la entrada y la salida.

Los dispositivos de control de acceso permitieron por medio de la configuración del módulo que el sistema los reconociera como objetos puerta y de acuerdo a esta se definió la conexión en la que se utilizaban. Cada lector se identificó directamente con el módulo al que estaba conectado, ligándolo a un área específica por medio del software y de esta forma relacionándolo al lugar preciso en donde se ubicó el control de acceso, esto se realizó con cada lector tanto en la entrada como la salida, identificándolos como pertenecientes a la misma puerta o al mismo sector. Al utilizar dispositivos de salida como el sensor RTE1000 o el interruptor, se indicó en la configuración del modulo AC-1 y así el sistema reconoció el cambio en la entrada donde se conectó este dispositivo. Adicionalmente, en la configuración fue posible establecer los tiempos, en

segundos, que el sistema debió esperar antes de que detectaran los eventos de puerta abierta o entrada forzada así como la duración de la señal que habilitó la cerradura, además de configurar el canal de la salida de la alarma del AC-1 y la duración de la misma.

Una vez configurado el sistema del control de acceso, las acciones relacionadas con este dispositivo generaron diferentes eventos que formaron parte de los atributos de los objetos a los que pertenecían, indicando la existencia de un acceso válido o inválido, un acceso con entrada, una solicitud de salida, puerta abierta o puerta forzada, esto se pudo observar en el cuadro de configuración de la puerta en AccessEvents, figura 6.5. Estos atributos variaban de acuerdo a las conexiones, y nos indicaban las acciones sin embargo, dado que el sistema por sí solo no cumplía con las necesidades de protección se requirió de la manipulación de los atributos mediante los programas de Plain English para optimizar el funcionamiento del sistema. Estas rutinas se diseñaron de acuerdo a cada conexión y a los atributos disponibles que se pudieran manipular.

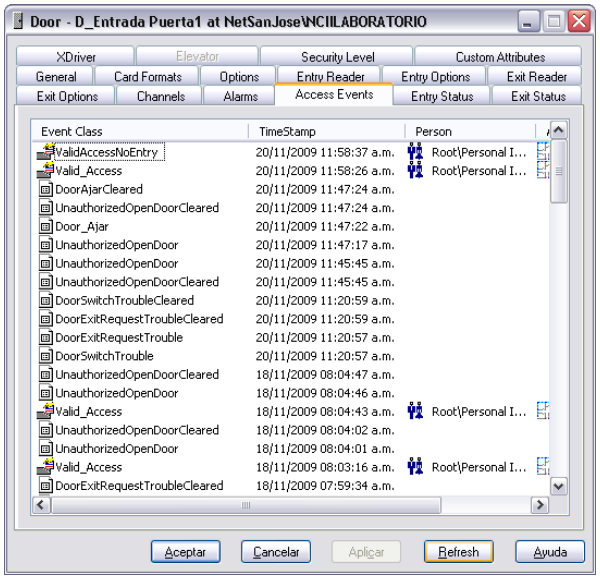



Figura 6.5 Cuadro de configuración de la Puerta1. Access Events.

La rutina inicial, en cualquiera de los tres casos del control de acceso, contempló el conteo de los ingresos, tomando en cuenta las veces que se reportó un acceso válido y si existió un cambio de estado en la entrada de los contactos magnéticos. Esta relación fue necesaria debido a que un acceso válido solamente implicó que la persona tenía autorización para ingresar, pero no si la persona ingresó, por tanto se dependió de ambos atributos para contabilizar un ingreso. En el conteo de salida se tuvo la diferencia entre los tres casos del control de acceso, los dos que involucraron un dispositivo de salida se evaluaron juntos debido a la similitud en el funcionamiento. Inicialmente se plateó una secuencia de conteo que se condicionó únicamente a la existencia de la solicitud de salida y al monitoreo de los terminales de los contactos magnéticos, sin embargo al realizar las pruebas con esta secuencia se presentaron dos problemas que afectaron el correcto funcionamiento del sistema y la fiabilidad, lo que obligó a modificar la rutina. Uno de estos problemas fue la forma en que el sistema procesaba la señal entrante del dispositivo que solicitó la salida, al detectarse el cambio en las entradas se identificó como una solicitud de salida y no como un acceso válido, el problema radicaba en que para que no se diera la alarma de puerta forzada, antes se debía detectar la existencia del acceso válido, al no darse esta condición cuando se daba la solicitud y se abría la puerta se activaban las alarmas, ya que se daba un cambio de estado en el atributo que indicaba que la puerta fue abierta sin autorización. El segundo problema se dio debido a la duración de la señal proveniente de los dispositivos de salida, ya fuera del interruptor, que dependió del tiempo en que el usuario lo mantuviera presionado, o bien del sensor, en donde el pulso menor tuvo una duración de 5s, ocasionando que la salida se contabilizara más de una vez por el sistema.

Como solución a la activación de la alarma de puerta forzada con la solicitud de salida se plantearon dos posibilidades, la primera supuso un horario de acuerdo al cual en horas laborales y de movimiento continuo esta alarma específicamente, se mantuviera desactivada, para luego retornar al monitoreo en

horas no hábiles como parte de las alarmas de intrusión, se realizó la prueba y el sistema respondió de forma favorable ya que la alarma no se activaba al abrir la puerta, pero tenía el inconveniente de que la puerta carecía de esta protección durante el día o las horas en que el personal autorizado estuviera laborando dentro del área respectiva, esto motivó al planteamiento de una segunda opción la cual se eligió de forma permanente. Esta segunda solución utilizó un temporizador que era activado al detectar la señal de la solicitud y cuya duración fue igual al tiempo que se envió la señal que habilitó la cerradura. Durante la ejecución de este temporizador se mantuvo activa una variable indicando la existencia de la solicitud y se desactivó la alarma de puerta forzada, permitiendo en ese momento que la puerta fuera abierta sin activar la alarma, sin embargo, si se abrió la puerta y esta permanecía abierta, una vez que pasó el tiempo establecido la alarma sonó, para solucionar esto se requirió de un segundo temporizador, el cual desactivó la alarma durante el mismo tiempo en que fue permitido mantener la puerta abierta. El motivo de utilizar dos temporizadores en lugar de uno solo que durara los dos tiempos juntos fue para evitar que si la salida no existió, el área quedara desprotegida durante ese tiempo.

Por otro lado se tuvo el problema de la duración del pulso entrante, para esto se incluyó dentro de la rutina una secuencia que detectara el primer conteo e ignorara los siguientes. Del primer temporizador de la rutina que desactivó la alarma, se tomó la variable que era activa al existir una solicitud y se monitoreó la entrada de los contactos magnéticos estableciendo esta variable y el atributo como las dos condiciones para el conteo de salida, una vez que se cumplieron las dos condiciones se contó una salida y se activó una variable de control que indicó que se contabilizó y por tanto se ignoró la señal hasta que entró la siguiente solicitud o el tiempo finalizó, evitando que se diera un recuento.

La conexión con el lector de proximidad a la salida presentó un problema similar al de la alarma forzada en la que se utilizaron los dispositivos de solicitud. En este caso aunque la señal del lector se identificó como un acceso válido, no

se reconoció como tal por el sistema, ya que en la entrada en donde debieron estar los contactos magnéticos no existía conexión alguna, por lo que al abrir la puerta el sistema lo procesó como una apertura no autorizada, activando la alarma de puerta forzada. El motivo de que no existiera esta conexión fue que los contactos magnéticos solo podían conectarse a uno de los AC-1, debido a que al conectarlos en ambos la impedancia de entrada en las entradas de los AC-1 variaba la impedancia equivalente afectando el circuito y la percepción en cada AC-1. Se eligió conectar los contactos magnéticos en el AC-1 correspondiente a la entrada para mantener una uniformidad en las secuencia de conteo de ingreso tanto para la conexión con dispositivos de salida como con lector. En cuanto a la duración de la señal no se presentó mayor problema debido a que era un pulso cuya duración no afectaba el conteo.

El problema de la alarma de puerta forzada de la conexión con lector a la salida se solucionó de la misma manera que en la que se usaban los dispositivos de salida. Es decir que la rutina utilizó dos temporizadores, uno que mantuvo activa la solicitud y desactivó la alarma de puerta forzada durante el tiempo que se habilitó la cerradura y el otro que desactivó la alarma durante el tiempo que se permitió mantener la puerta abierta. Para el conteo de salida solo se monitoreó la apertura de la puerta y se verificó la existencia de la solicitud.

En la rutina de conteo se incluyó el monitoreo de los sensores, con una variable utilizada como bandera que indicaba la inactividad en el área. Esto debido a que esta secuencia en conjunto con el contador fueron las condiciones que determinaron el arme o desarme de las alarmas del control de intrusión.

La siguiente rutina se encargó del monitoreo. La ejecución de esta rutina se condicionó a dos variables que dependieron de la rutina de conteo, el contador y la bandera de inactividad. Si se cumplió con alguna de estas dos condiciones se iniciaba la secuencia. Esto se determinó así al considerar que era innecesario que el monitoreo se estuviera ejecutando de forma continua si en realidad su

función era detectar que ya no había actividad o personal dentro del área y por tanto iniciar el protocolo para armar los dispositivos de alarma.

El protocolo para armar las alarmas consistió en que una vez que se identificó inactividad o bien el contador en cero, el control debió otorgar un tiempo para permitir que si alguna persona quedó dentro saliera del área y posterior a esto el programa decidió respecto a las alarmas que ejecutaría. Este último punto se incluyó por si se daba el caso de que aunque el contador marcara cero los sensores continuaran detectando movimiento, con esto se indicaba que había una o más personas dentro sin estar registrados en el contador del sistema, de acuerdo a esto se activó una alarma preventiva que envió una notificación indicando la presencia de esas personas, si por otro lado pasado el tiempo los sensores indicaron inactividad se armaron las alarmas respectivas, esto se realizó por medio de una bandera que indicó la autorización para iniciar la rutina de las alarmas.

La rutina de alarmas monitoreó cada una de las entradas del DI-8 en las que se conectaron sensores, si cambió el estado de alguna de estas entradas se tomó como el inicio de la secuencia de la alarma. La misma funcionó con un temporizador cuya duración podía modificarse y cambió la salida de los DO-4 de manera que se pudo variar la frecuencia del sonido en la salida de la alarma, si esta constaba de un dispositivo sonoro. Además fue posible establecer una alarma silenciosa que solamente envió la notificación a la estación de trabajo.

Las notificaciones y los registros de alarma también se configuraron dentro del CyberStation, y cada uno de estos fue personalizado de acuerdo a las necesidades del área a la que estaban ligados. Estas alarmas aparecieron en la barra de alarmas de la pantalla principal de CyberStation, figura 6.6 o en el visor de alarma figura 6.7.


Figura 6.6 Barra de alarmas de CyberStation.

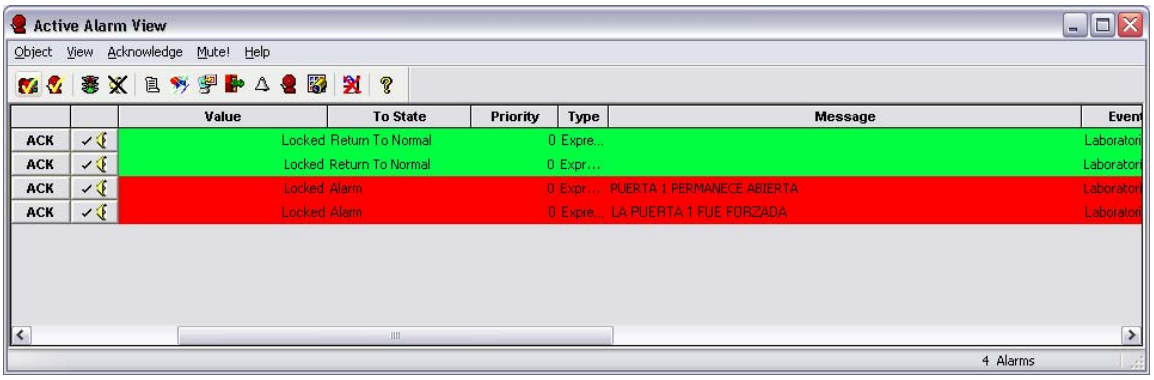



Figura 6.7 Visor de alarmas de CyberStation.

Las notificaciones indicaron que procedimiento se debió seguir al darse la alarma como el envío de mensajes a la barra de alarmas del CyberStation en la estación de trabajo de manera silenciosa o incluyendo un sonido de alarma entre otros, así se identificó además que estaciones de trabajo serían receptores de estas alarmas. Los registros de alarma ligaron la notificación con la variable o el atributo que accionaba la alarma.

El conjunto formado por el módulo de pruebas y las rutinas ejecutadas formaban el sistema integral de seguridad, el mismo a través de las aplicaciones permitió la interacción entre el control de acceso y los dispositivos de entrada y salida obteniendo un mismo sistema que permitía determinar mediante los parámetros de ocupación y permanencia del personal el arma y desarme del control de intrusión. Por medio de los contadores era posible conocer el movimiento que existía en los diferentes sectores.

Analizando de cerca las conexiones del control de acceso que se utilizaron, fue posible identificar las ventajas de la configuración con un lector en la entrada y la salida con respecto a la que se implementó con dispositivos de solicitud de salida. Esta ventaja se centró principalmente en que era obligación del usuario identificarse tanto en la entrada como en la salida lo que permitió obtener un

mayor control en el acceso a esa área, por el contrario con el dispositivo de salida no fue posible identificar la persona o personas que salieron, lo que le restó confiabilidad al contador que llevó el registro de estos movimientos. Cabe mencionar que aunque el contador no identificó a la persona que entraba o salía, el evento quedó registrado en los accesos de cada puerta con la identificación respectiva y almacenada en la base de datos del sistema.

# Capítulo 7. Conclusiones y recomendaciones

## 7.1. Conclusiones

- El hardware de la plataforma Andover Continuum permitió la interacción con otros dispositivos, debido a la versatilidad de sus módulos de entrada y salida, así como las características eléctricas de estos, que no requirieron de circuitos adicionales para el acople.
- La configuración de los módulos proporcionó la definición de las funciones específicas que debieron cumplir cada uno de forma individual, brindando un conocimiento directo del sistema y los eventos involucrados para su oportuna manipulación o modificación a través de aplicaciones en Plain English.
- Plain English como lenguaje basado en la programación orientada a objetos facilitó la interacción con los módulos y cada una de sus entradas, salidas, atributos y características, logrando enlazar el sistema en un control único
- La escalabilidad del sistema permitió el desarrollo de un módulo de pruebas o prototipo que lo recreó en un espacio reducido de manera que pudo utilizarse para pruebas y análisis.
- El módulo de pruebas incluyó los tres escenarios en que se utilizó el control de acceso y los dispositivos del control de intrusión.
- La conexión del control de acceso con identificación en la entrada y la salida brindó una mayor confiabilidad, ya que obligó al personal a identificarse y por tanto el conteo registró todos los movimientos.
- Los contadores de los accesos llevaron un control numérico de los movimientos, no así de las identidades del individuo en cada evento, aunque este dato si quedó almacenado en la base de datos.
- Por medio de las rutinas del control de acceso se manejaron los dispositivos del control de intrusión.

## 7.2. Recomendaciones

El Sistema de Gestión Andover Continuum dispone del hardware necesario para aumentar las aplicaciones, pudiendo ser utilizado con sensores analógicos para control de otros procesos como el despacho de combustible o bien ambientación en lugares específicos que tengan que mantener ciertas normas de seguridad, así como sistemas para control de activos.

Adicionalmente se puede controlar el sistema de cámaras o circuito cerrado de televisión para aumentar la vigilancia, enlazándolo con los controles de eventos de forma que puedan ser utilizados en conjunto para la atención de eventos o alarmas.

## Capítulo 8. Bibliografía


1. Andover Continuum Configurator's Guide for Version 1.8. 2006.
2. Andover Continuum CyberStation Plain Language Reference. 2006
3. Andover Continuum I/O Modules. 2006
4. Andover Continuum I/O System Reference. 2006
5. Andover Continuum Power Supply Reference. 2006
6. Automatización de edificios. Consultado el 28 de setiembre de 2009 de http://www.schneiderelectric.es/sites/spain/es/solutions/energy_efficiency/by-application/automatizacion-de-edificios.page
7. Edificios inteligentes. SicaNews. Consultado el 28 de setiembre de 2009 de http://www.paginadigital.com.ar/ARTICULOS/2002rest/2002terc/tecnologia/sica98.html
8. Márquez García-Cuervo, Diego. Protocolo Wiegand. Consultado el 28 de setiembre de 2009 de http://www.ucontrol.com.ar/wiki/index.php/El_protocolo_Wiegand.
9. NetControler II CPU Module. 2006
10. NetController II Operational and Technical Reference Guide. 2006
11. RFID. Consultado el 28 de setiembre de 2009 de http://es.wikipedia.org/wiki/RFID

# Capítulo 9. Apéndices

## 9.1. A.2 Manual de usuario

# Capítulo 10. Anexos

## Atributos de puerta [2]

Door Attributes

Door Attributes Table continued

| Attribute | Description |
|---|---|
| DoorAjar | Indicates that the door has been left open too long |
| DoorAjarTime | Time required for door to be considered ajar |
| DoorChannel | Terminal number into which this object is wired |
| DoorFault | True/false depending on status of supervised input |
| DoorSchedule | Name of the schedule attached to this door |
| DoorStrikeTime | Time duration of relay activation on door open command |
| DoorSwitch | Indicates if a door switch input is used |
| DoorSwitchChan | Terminal number into which this object is wired |
| DoorSwitchType | Wiring type - NOSeries, etc. |
| Duress | Indicates if duress notification is to be used |
| EditLock | Indicates if object has been locked to additional Edits |
| EntEgrViol | Indicates if there is an entry/egress violation |
| EntryNormMode | Indicates if entry took place in normal mode |
| EntryNotReentry | Indicates if entry took place with no reentry permitted |
| EntryPinDuress | Indicates if entry via pin was duress |
| EntryRvrsCrdDur | Indicates if entry via reverse card was duress |
| EntrySchedule | Schedule attached to the entry reader |
| EntryZone | Zone entered through entry reader |
| ExitAntiPassTime | Time required for passback through this door to be permitted |
| ExitArea | Area entered from exit reader |
| ExitChannel | Terminal number into which this object is wired |
| ExitCount | Number of people who have exited |
| ExitEntEgr | |
| ExitEntrAntiPass | |
| ExitEntrEntEgr | |
| ExitEntrRvrsCrd | Allow entry through exit door on reverse card |
| ExitIOU | IOU number of object |
| ExitKyPdChan | Terminal number into which this object is wired |
| ExitLastCard | Last card number have valid access through exit reader |
| ExitLastSite | Site code of last card number have valid access through exit reader |
| ExitMode | Mode of Exit reader |
| ExitNoCommMode | Exit reader in nocomm mode |
| ExitNoDataMode | Exit reader in no data mode - no communication with access server |
| ExitNoReentry | Indicates if exit took place with no reentry |

## Door Attributes

Door Attributes Table continued

| Attribute | Description |
|---|---|
| ExitNormMode | Indicates exit in normal mode |
| ExitPinDuress | Indicates exit with pin duress |
| ExitRequest | Indicates the presence of PIR or some form exit request sensor |
| ExitRequestChan | Terminal number into which this object is wired |
| ExitRequestType | Wiring type - NCSeries, etc. |
| ExitRvrsCrdDur | Indicates exit via a reverse card duress signal |
| ExitSchedule | Schedule attached to the exit reader |
| ExitZone | Zone entered when going through the exit reader |
| Export | Indicates that the object value has been tagged for export. |
| FollowUpRule | Not Meaningful to the User |
| ForcedEntry | Indicates that the door has been forced open |
| GeneralCode | |
| Graphics | Not Meaningful to the User |
| IconID | Not Meaningful to the User |
| ID | SQL Object ID - Not Meaningful to the User |
| ExitEntrRvrsCrd | Allow entry through exit door on reverse card |
| IncludeObject | Not Meaningful to the User |
| InvalidAttempt | Indicates an invalid card was used |
| InvalidEntryTime | Indicates an attempt to enter before proper antipassback time has elapsed |
| InvalidExitTime | Indicates an attempt to exit before proper antipassback ime has elapsed |
| Invert | Revers Polarity |
| LastChangeBy | Name of the user making the last change |
| LastDepEntdPnt<br>LastDepExitdPnt | |
| LastInvalidEntry | Last invalid card swiped at entry reader |
| LastInvalidExit | Last invalid card swiped at exit reader |
| LastPersonEntrd | Last cardholder entering door |
| LastPersonEntrdDep | Department number of last person entered |
| LastPersonExitd | Last person with valid swipe at the exit reader |
| LastPersonExitdDep | Department number of the last person with valid swipe at the exit reader |
| LCDSettable | Capable of being set from the LCD |
| LockedBy | Not Currently Implemented |

## Door Attributes

Door Attributes Table continued

| Attribute | Description |
|---|---|
| LockingWorkstation | Not Currently Implemented |
| Name | Name of the object |
| NetworkNumber | Not Meaningful to the User |
| OpenOnExitRequest | Indicates that door to be opened upon sensing exit request on exit request input |
| OperatingMode | Current operating mode of the door |
| Override | Indicates if the door has been overridden in the field |
| OverrideValue | Indicates the true value of the door when it has been overridden in the field |
| Owner | Object that owns this door object |
| Param1....Param6 | XDriver configuration value |
| Port | Comm port associated with Xdriver |
| Properties | Not Meaningful to the User |
| RecordDrAjarHist | Keep access event history for door ajar |
| RecordExitRqHist | Keep access event history for exit requests |
| RecordForcedHist | Keep access event history for forced entries |
| RecordInvalHist | Keep access event history for invalid attempts |
| ReferencePoint1... ReferencePoint4 | Alarm Reference Point |
| Refresh | Rebroadcasts current value of point |
| RefTemplate | Name and path of template from which object was created |
| RelockOnClose | Relock as soon as sensor indicates closed, do not wait for strike time to elapse |
| ReportID | Not Meaningful to the USer |
| ScheduleEvents | Not viewable by user |
| SecurityLevel | Name and path of any security level attached to the object |
| Site1...Site4 | Site code that can be used by readers |
| State | Indicates if an object has been enabled or disabled |
| Template | When true, indicates that object was made from a template |
| TemplateAlias | Alias that will be used when creating objects from this template object - meaningful only for templates |
| TemplateCreateRule | Not meaningful to user |
| TemplateName | Name that will be used when creating objects from this template object - meaningful only for templates |
| TimeEntered | Last time a swip occurred on exit reader |
| TimeExited | Last time a swip occurred on entry reader |
| TimeLocked | The time the object was last opened |

## Door Attributes

Door Attributes Table continued

| Attribute | Description |
|---|---|
| Type | The type of the object |
| UnlockSchedule | Schedule attached to unlock door |
| ValidAccess | Indicates a valid access through door |
| Value | The value of this object after any conversions that may be required |